MAANPUOLUSTUSKORKEAKOULU

MENETELMIÄ JOUKON ELEKTRONISEN AKTIIVISUUDEN ARVIOIMISEKSI - INFORMAATIOTEOREETTINEN NÄKÖKULMA

Diplomityö

Kapteeni
Pekka Passinen

Yleisesikuntaupseerikurssi 55
Ilmasotalinja

Heinäkuu 2011

MAANPUOLUSTUSKORKEAKOULU

Kurssi	Linja
Yleisesikuntaupseerikurssi 55	Ilmasotalinja

Tekijä

Kapteeni Pekka Passinen

Tutkielman nimi

MENETELMIÄ JOUKON ELEKTRONISEN AKTIIVISUUDEN ARVIOIMISEKSI - INFORMAATIOTEOREETTINEN NÄKÖKULMA

Oppiaine, johon työ liittyy	Säilytyspaikka
Sotatekniikka	Kurssikirjasto (MPKK:n kirjasto)
Aika Heinäkuu 2011	Tekstisivuja 120 Liitesivuja 37

Tiivistelmä

Sähkömagneettista spektriä hyödynnetään laajasti erilaisten tietoliikenne- ja sensorijärjestelmien lähettämän datan siirtotienä. Tätä siirrettävää dataa hyödynnetään sotilasjoukon johtamisessa ja tilannekuvan muodostamisessa. Siinä, missä sotilasjoukko saa merkittävää hyötyä sähkömagneettisen spektrin käytöstä, se myös samalla tuottaa informaatiota joukon toiminnasta kiinnostuneen tiedustelijan ulottuville. Tiedustelija pyrkii elektronisen tiedustelun menetelmin havaitsemaan ja hyödyntämään mahdollisimman tehokkaasti ulottuvilleen päätyvän informaation. Sotilasjoukon on kyettävä kontrolloimaan omaa elektronista aktiivisuuttaan siten, että tiedustelujärjestelmän kyky tuottaa tilannekuvaa voidaan kiistää tai ainakin tiedustelijan ulottuville päätyvän informaation määrä on ennakoitavissa.

Ennakointia ja erilaisten olosuhteiden vertailua varten tarvitaan menetelmiä, joilla kyetään yksiselitteisesti ja mitallisesti arvioimaan joukon sisältämän ja tuottaman sekä tiedustelijan saataville päätyvän informaation määrää. Näiden menetelmien kehittäminen on tämän tutkimuksen päämäärä. Informaatioteoria tarjoaa työkaluja informaation määrän arvioimiseksi ja on näin ollen varsin luonnollinen valinta tutkimuksen näkökulmaksi.

Tuloksina esitellään neljä erillistä menetelmää, joita voidaan hyödyntää joukon elektronisen aktiivisuuden ja elektronisen suojautumisen tason arvioinnissa. Menetelmistä kaksi mittaa joukon sisältämää informaatiota eli organisaatioon sijoitettujen lähettimien jakautumista ja erottuvuutta ympäristöstään. Kaksi muuta menetelmää keskittyvät analysoimaan joukon tuottaman (lähettimien käyttötapoihin liittyvää) informaation määrää ja sen päätymistä tiedustelijan ulottuville erilaisissa olosuhteissa. Kehitetyt menetelmät perustuvat entropian, ehdollisen entropian, yhtenäisinformaation, suhteellisen entropian ja informaation yhteenlaskettavuuden määritelmiin ja ominaisuuksiin. Oleellinen osa työtä on joukon lähettimien käytön mallintaminen stokastisten prosessien avulla sekä erilaisten häiriöiden huomioiminen.

Menetelmien hyödynnettävyyden osalta voidaan osoittaa, että menetelmät tarjoavat selkeitä mitallisia ja entistä monipuolisempia mahdollisuuksia arvioida erilaisia olosuhteita elektronisen suojautumisen kannalta. Vaikka menetelmät jäävä varsin teoreettiselle asteelle, on varsin selkeästi havaittavissa niiden tarjoamat mahdollisuudet tuottaa lisäarvoa joukon toimintavaihtoehtojen vertailuun ja operaatioanalyyttisiin tarkasteluihin. Käytännöllisten työkalujen kehittäminen vaatii kuitenkin jatkotutkimusta ja kehitystyötä.

AVAINSANAT
Elektroninen Sodankäynti (ELSO), elektroninen suojautuminen (ELSU), elektroninen tiedustelu, elektroninen tuki (ELTU), informaatioteoria, informaatio, entropia

KIITOKSET

Kiitän työn ohjaajia TkL Antti Rissasta ja FT Juhani Hämäläistä.

Kiitokset myös FT Matias Aunolalle muutamista työn visuaalista ilmettä ja rakennetta parantaneista vinkeistä.

Lopuksi kiitokset vaimolleni Teijalle ja pojalleni Samille.

Santahaminassa 27.7.2011

Pekka Passinen

MENETELMIÄ JOUKON ELEKTRONISEN AKTIIVISUUDEN ARVIOIMISEKSI - INFORMAATIOTEOREETTINEN NÄKÖKULMA

SISÄLLYSLUETTELO

LYHENTEET, SYMBOLIT JA KÄSITTEISTÖÄ

LYHENTEET, SYMBOLIT JA KÄSITTEISTÖÄ

Seuraavassa on esitelty yleisimmät työssä käytetyt lyhenteet ja symbolit. Lisäksi on lyhyesti esitelty keskeisiä tekstissä esiintyviä matemaattisia käsitteitä. Niiltä osin, kuin lyhenteitä, symboleita tai käsitteitä ei ole sisällytetty tähän osioon, ne on esitelty tekstiosassa.

Työssä yleisimmin käytetyt lyhenteet.

AM	Amplitude Modulation, amplitudimodulaatio
bit	bitti
COMINT	Communication Intelligence, viestitiedustelu
dB	desibeli
dBm	desibelimilliwatti
EA	Elektronic Attack, elektroninen vaikuttaminen
ELINT	Electronic Intelligence, elektroninen mittaustiedustelu
ELSO	elektroninen sodankäynti
ELSU	elektroninen suojautuminen
ELTU	elektroninen tuki
ELVA	elektroninen vaikuttaminen
EMCON	Emission Control, emissioiden hallinta
EP	Electronic Protection, elektroninen suojautuminen
ES	Electronic Support, elektroninen tuki
esim.	esimerkiksi, esimerkki
et. al.	lat. *et alii*, ja muut, ynnä muut
e-SIGINT	Data-network Intelligence, dataverkkojen signaalitiedustelu
FDMA	Frequency Division Multiple Access, taajuusjakoinen monikanavointi
FISINT	Foreign Instrumentation Signals Intelligence, vieraiden laitteiden tiedustelu
FM	Frequency Modulation, taajuusmodulaatio
FSK	Frequency Shift Keying, taajuusavainnus
GHz	gigahertsi
HF	High Frequency
HPM	High Power Microwave
Hz	hertsi
jne.	ja niin edelleen
kHz	kilohertsi
km	kilometri
ko.	kyseessä oleva
kpl	kappaletta
ks.	katso
lkm.	lukumäärä
LPD	Low Probability of Detection. Signaali tai järjestelmä, jonka lähete on vaikeasti ilmaistavissa.
LPI	Low Probability of Intercept. Signaali tai järjestelmä, jonka lähete on vaikeasti siepattavissa.
m^2	neliömetri
max	maksimi
merk.	merkitään
MHz	megahertsi

ml.	mukaan luettuna, mukaan luettuina
mm.	muun muassa
n.	noin
ns.	niin sanottu
PM	Phase Modulation, vaihemodulaatio
PSK	Phase Shift Keying, vaiheavainnus
rms	Root Mean Square, neliöllinen keskiarvo
s.	sivu, sivut, sivuilla
s	sekunti
sek	sekunti
SIGINT	Signal Intelligence, signaalitiedustelu
symb	symboli
TDMA	Time Division Multiple Access, aikajakoinen monikanavointi
ts.	toisin sanoen
tv	televisio
UHF	Ultra High Frequency
vast.	vastaava, vastaavasti
VHF	Very High Frequency
vrt.	vertaa

Yleisimmät työssä käytetyt symbolit ja niiden käyttötarkoitukset.

B	kanavan kaistanleveys
c_{ij}	kuvautumistodennäköisyys
C	kanavan kapasiteetti
D	tiedustelujärjestelmän kapasiteetti, yleismerkintä
D_{KL}	suhteellinen entropia
$D_{KL}(P \parallel Q)$	suhteellinen entropia todennäköisyysjakaumien P ja Q välillä
D_M	tiedustelujärjestelmän absoluuttinen kapasiteetti
D_N	tiedustelujärjestelmän normalisoitu kapasiteetti
D_R	tiedustelujärjestelmän suhteellinen kapasiteetti
E_E	tyypillistä taistelutilannetta vastaava emissioympäristö
E_U	tasajakaumaan perustuva emissioympäristö
H	entropia
H_s	diskreetin informaation lähteen entropia [bit/symb]
H_s'	diskreetin informaation lähteen entropian nopeus [bit/sek]
H_{sE}	tyypillistä taistelutilannetta kuvaavan emissiomallin entropia
H_{sU}	tasajakaumaa noudattelevan emissiomallin entropia
$H(X)$	satunnaismuuttujan X entropia, joukon X entropia
$H(Y)$	satunnaismuuttujan Y entropia, joukon Y entropia
$H(X,Y)$	satunnaismuuttujien X ja Y yhteisentropia
$H(X\|Y)$	satunnaismuuttujan X ehdollinen entropia kun Y tunnetaan
$H(Y\|X)$	satunnaismuuttujan Y ehdollinen entropia kun X tunnetaan
$H(\cdot \mid \cdot)$	ehdollinen entropia, yleismerkintä
$H_1(P)$	1-asteen entropia todennäköisyysjakaumalle P
I	yhtenäisinformaatio, yleismerkintä Joissain yhteyksissä (ks. esim. [19]) käytetty termi keskinäisinformaatio tarkoittaa samaa, kuin tässä työssä käytetty yhtenäisinformaatio.
$I(X;Y)$	satunnaismuuttujien X ja Y välinen yhtenäisinformaatio
Ln	lähetekategorian tunnus
p_i	tilastollinen todennäköisyys, esiintymistodennäköisyys

$p(x_i)$	symbolin x_i tilastollinen todennäköisyys, käytetään usein esiintymistodennäköisyytenä
$p(y_j)$	symbolin y_j tilastollinen todennäköisyys, käytetään usein vastaanottotodennäköisyytenä
$p(x_i, y_j)$	symbolien x_i ja y_j yhteistodennäköisyys
$p(x_i\|y_j)$	x_i:n ehdollinen todennäköisyys kun y_j tunnetaan
$p(y_j\|x_i)$	y_j:n ehdollinen todennäköisyys kun x_i tunnetaan
P_D	ilmaisutodennäköisyys
P_{DR}	ilmaisusuhde
P_{EX}	hyödyntämistodennäköisyys
P_H	havaitsemistodennäköisyys
P_{ij}	siirtymätodennäköisyys tilojen i ja j välillä
P_K	käytettävyystodennäköisyys
P_L	lähetetodennäköisyys, yleismerkintä
P_{Ln}	lähetetodennäköisyys lähetekategorian Ln lähettimille
P_{POI}	sieppaustodennäköisyys
R	informaation lähteen lähetysnopeus
S_0^{Ln}	lähetekategoriaan Ln kuuluvien lähettimien kokonaislukumäärä joukossa
S/N	signaali-kohina suhde
v_j	vastaanottotodennäköisyys
$W(P)$	todennäköisyysjakauman P painokerroin
δ	paikannustarkkuutta mallintavan ympyrän säde
Δ	tiedustelujärjestelmän ja kohteena olevan lähettimen välinen etäisyys
ε	todennäköisyysjakaumien välisen epäsovituksen raja-arvo
μ_i	rajatodennäköisyys symbolille i, indeksinä käytetty myös merkintää j
μ	Markov prosessin vakaa todennäköisyysjakauma
$\pi(\alpha_i)$	tarkasteltavalla alueella sijaitsevan symbolin α_i esiintymistodennäköisyys
ρ_D	tiedustelutodennäköisyysjakauma
ρ_h	tiedustelutodennäköisyysjakauma hetkellä h (h = emissiomallin tuottamien symboleiden lukumäärä).
ρ_i	tiedustelutodennäköisyys
φ	symbolinopeus, yleismerkintä
φ_i	emissiomallin tilaa i vastaava symbolinopeus
φ_{avg}	keskimääräinen symbolinopeus
$\forall$	kaikille
$\exists$	on olemassa
$\in$	kuuluu joukkoon
$\notin$	ei kuulu joukkoon
$\subset$	sisältyy joukkoon (aitona osajoukkona)
$\varnothing$	tyhjä joukko
$\mapsto$	kuvautuu
■	todistettu
◊	merkintää käytetään ilmaisemaan tekstiin sijoitetun esimerkin tai määritelmän loppua

Todennäköisyyslaskentaan liittyvää käsitteistöä.

Tämän työn tarkastelut pohjautuvat tilastolliseen todennäköisyysmallinnukseen, joka edellyttää satunnaismuuttujan ja todennäköisyysmassan jakautumista ko. satunnaismuuttujalle kuvaavan todennäköisyysjakauman olemassaoloa. Diskreetillä todennäköisyysmassafunktiolla voidaan kuvata tätä todennäköisyysmassan jakautumista satunnaismuuttujan eri arvoille. Työssä käsitellään vain diskreettejä todennäköisyysmassafunktioita, joista on monissa kohdin käytetty yksinkertaisesti diskreetin todennäköisyysjakauman tai vain todennäköisyysjakauman nimitystä.

Ehdollisilla todennäköisyyksillä on merkittävä asema esiteltävissä tarkasteluissa. Ehdollinen entropia voidaan määrittää kahden toisistaan jollain tavalla riippuvan tapahtuman välille seuraavasti

$$P(A \mid B) = \frac{P(AB)}{P(B)} = \frac{P(B \mid A)P(A)}{P(B)}.$$

Yllä oleva lauseke ilmaisee todennäköisyyden tapahtumalle A silloin, kun tapahtuma B on tapahtunut ensin. Lisäksi havaitsemme ko. lausekkeesta, että tapahtumien A ja B yhteistodennäköisyys on

$$P(AB) = P(A \mid B)P(B) = P(B \mid A)P(A).$$

Todennäköisyyslaskennan perusteista on löydettävissä runsaasti kirjallisuutta. Tässä työssä käytetystä kirjallisuudesta lisätietoja ko. aiheesta löytyy mm. [46], [53], [56] ja [57].

Entropiaan liittyvää käsitteistöä.

Entropialle käytetään merkintää $H(X)$, jossa sulkeissa oleva symboli tarkentaa, minkä satunnaismuuttujan (joukon) suhteen entropia on laskettu. Joissain kohdin sulkeiden sisällä käytetään todennäköisyysjakauman merkintää esim. $H(P)$, joka siis ilmaisee minkä todennäköisyysjakauman suhteen entropia lasketaan. Merkintöjen poikkeavuudesta huolimatta kyse on samasta käsitteestä.

MENETELMIÄ JOUKON ELEKTRONISEN AKTIIVISUUDEN ARVIOIMISEKSI - INFORMAATIOTEOREETTINEN NÄKÖKULMA

1. JOHDANTO

1.1. Johtolankoja spektrissä

Sähkömagneettisen spektrin käyttö on etuoikeus, jota nykyaikainen ihminen hyödyntää niin yksilöllisellä kuin yhteisöllisellä tasolla. Myös sotilasjoukolle sähkömagneettisen spektrin käyttö on etuoikeus, jolla on jo noin vuosisadan [58, s. 110 – 113] ajan nopeutettu tilannetietoisuuden kehittymistä ja johtamista. Tällä etuoikeudella on myös hintansa; siinä missä spektrin käyttö nopeuttaa omaa toimintaa, se myös tarjoaa vastustajalle mahdollisuuden tilannetietoisuutensa parantamiseen. Sotilasjoukko jättää toiminnastaan johtolankoja sähkömagneettiseen spektriin. Elektroninen tiedustelu pyrkii löytämään nämä johtolangat ja rakentamaan niistä mahdollisimman tarkasti todellisuutta vastaavan tilannekuvan.

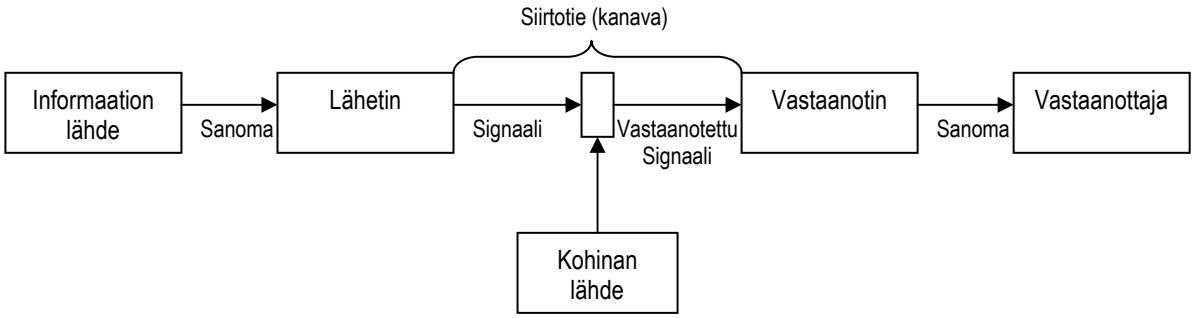
Sotilasjoukon on siis oltava tarkka ja ovela, jotta johtolangat eivät ole liian ilmeisiä. On huolehdittava siitä, että oma elektroninen aktiivisuus on panos-tuotos suhteeltaan toimintaan nähden oikeanlainen; elektronisen aktiivisuuden on hyödynnettävä omaa joukkoa enemmän kuin vastustajaa. Elektronisen suojautumisen huomioimisella pyritään saavuttamaan suhteellinen etu vastustajaan nähden. Sotilasjoukon on kyettävä arvioimaan omaa toimintaansa ja toimintavaihtoehtojaan myös näistä näkökulmista. Tämän työn tueksi tarvitaan sopivia työkaluja.

Tyypillinen työkalu tämän kaltaisia analyyseja varten on radioaaltojen etenemistä kuvaava laskentamalli ja sitä hyödyntävä tietokoneohjelma [30, s. 101]. Tällöin keskitytään erityisesti tarkastelemaan, millaisilta etäisyyksiltä joukon spektriin jättämät johtolangat on kerättävissä. Tällainen menetelmä ei kuitenkaan analysoi yksittäisen johtolangan merkitystä ja hyödynnettävyyttä tiedustelijan näkökulmasta. Tiedustelijan näkökulma tarkoittaa, että käsitys todelli-

suudesta muodostetaan perustuen vain niihin johtolankoihin, jotka on saatu kerättyä. Osa johtolangoista on voinut hävitä tai osa niistä on epäselviä. Tiedustelun kohteena oleva joukko on myös voinut piilottaa osan johtolangoista siten, että ne eivät koskaan päädy tiedustelijan ulottuville. On siis arvioitava, kuinka paljon informaatiota tiedustelijan käyttöön päätyneet johtolangat sisältävät verrattuna kaikkien johtolankojen sisältämään informaatioon. Informaation määrää tulee siis kyetä mittaamaan jollain menetelmällä. Luonnollinen lähestymistapa tämän kaltaisiin ongelmiin on etsiä sopivia työkaluja informaatioteoreettisten määritelmien joukosta.

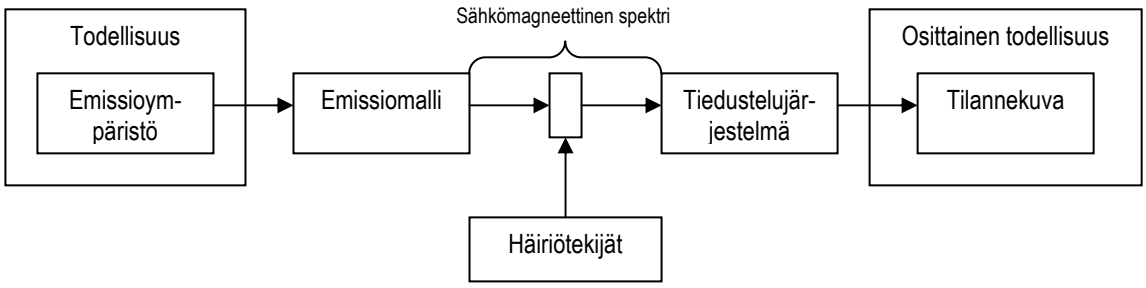
1.2. Informaatioteoreettinen näkökulma ja tutkimuksen tavoitteet

Motivaationa informaatioteoreettiselle näkökulmalle on toiminut A. Bordenin artikkeli [10], jossa esitetään, että elektronisen sodankäynnin ja informaatiosodankäynnin tärkeimmät periaatteet voidaan johtaa klassisista Claude E. Shannonin määritelmistä [62] informaatiolle ja kommunikaatiolle (communication). Kuvassa 1.1 on esitetty Shannonin alkuperäinen määritelmä informaatiota siirtävän (kommunikoivan) järjestelmän rakenteesta. Tarkemmat informaatioteoreettiset perusteet on esitelty luvussa 3.



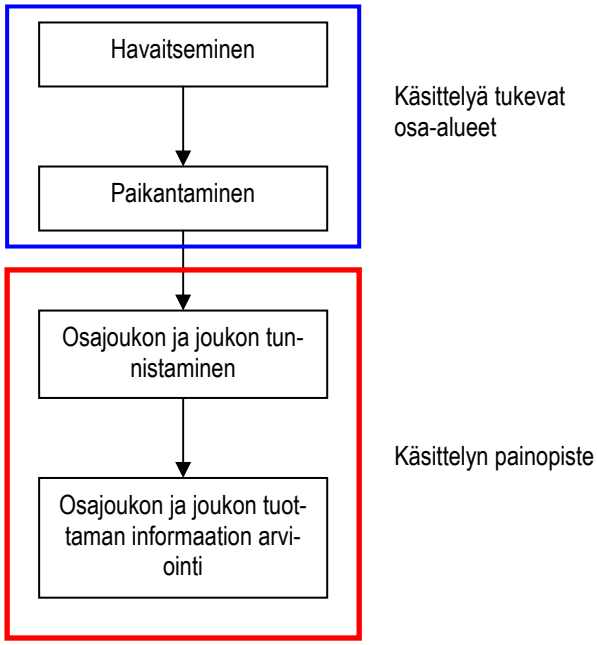
Kuva 1.1: Yleiskuvaus informaatiota siirtävästä järjestelmästä [62, s. 2].

Tässä työssä informaatiota siirtävän järjestelmän rakennetta sovelletaan kuvan 1.2 mukaisesti. Informaatiota tuottaa todellinen emissioympäristö, joka sisältää joukolle kuuluvat sähkömagneettista säteilyä lähettävät laitteet. Informaatio tuotetaan kanavalle emissiomallissa määriteltyjen sääntöjen mukaisesti. Kanavana toimii sähkömagneettinen spektri, josta tiedustelujärjestelmä pyrkii keräämään emissioympäristön tuottaman informaation. Erilaiset tekniset, fysikaaliset ja toiminnalliset häiriötekijät kuitenkin vaikeuttavat informaation keräämistä. Näin ollen lopputuloksena on tilannekuva, joka vastaa todellisuutta yleensä vain osittain. Tämän tutkimuksen tarkoituksena on etsiä menetelmiä, joiden avulla voidaan arvioida, kuinka erilaiset olosuhteet ja toimenpiteet vaikuttavat tiedustelijan muodostamaan tilannekuvaan.



Kuva 1.2: Todellisuuden kuvautuminen tiedustelujärjestelmän tuottamaksi tilannekuvaksi.

Elektronisen tiedustelun päämääränä on havaita, tunnistaa, paikantaa ja analysoida ympäristössä esiintyvät sähkömagneettista säteilyä lähettävät lähettimet [61]. Näiden vaiheiden kautta syntyy tiedustelujärjestelmän tuottama tilannekuva. Näistä vaiheista on löydettävissä myös tämän työn painopistealueet ja tukevat tekijät. Kuvassa 1.3 on havainnollistettu käsittelyn painopistealueita ja tukevia osa-alueita. Lähetteiden havaitseminen ja paikantaminen otetaan huomioon elektronisen aktiivisuuden ja elektronisen suojautumisen arviointiin soveltuvia menetelmiä määriteltäessä, mutta näihin osa-alueisiin liittyvät yksityiskohdat jätetään varsin kevyelle käsittelylle.



Kuva 1.3: Käsittelyn painopiste.

Elektronisella aktiivisuudella ymmärretään joukon tai sen osan (osajoukon) ominaisuuksia, käyttötapoja ja intensiteettiä sähkömagneettisen spektrin näkökulmasta tarkasteltuna. Elektronisen aktiivisuuden arviointi voidaan jakaa kahteen kokonaisuuteen:

- osajoukon ja joukon sisältämän informaation arviointi
- osajoukon ja joukon tuottaman informaation arviointi.

Joukon sisältämällä informaatiolla ymmärretään tässä käsittelyssä joukon sisältämien sähkömagneettista säteilyä lähettävien laitteiden jakaumaa organisaation sisällä. Joiltain osin voidaan sivuta myös käyttöperiaatteita. Tämä laitejakauma sisältää informaatiota, jota tiedustelija voi käyttää hyväkseen luokitellessaan ja tunnistaessaan joukon osia ja toimintaa. Tavoitteena on löytää menetelmiä, joilla joukon ja organisaation arviointi on tästä näkökulmasta mahdollista.

Joukon tuottama informaatio liittyy ennen muuta tapaan, jolla erilaisia lähettimiä käytetään. Nämä tavat vaikuttavat suoraan siihen, miten paljon informaatiota tuotetaan tiedustelijan saataville. Tavoitteena on löytää menetelmiä, joilla voidaan ensinnäkin kuvata näitä lähettimien käyttötapoja ja toisekseen menetelmiä, joilla voidaan arvioida tuotetun informaation määrää erilaisissa olosuhteissa.

Esiteltyihin näkökulmiin, painopisteisiin ja tavoitteisiin sitoen, tutkimuskysymykset asetetaan seuraavasti:

1) Millaisia menetelmiä on löydettävissä osajoukon elektronisen aktiivisuuden arvioimiseksi?
    - Miten osajoukon tunnistettavuutta / erottuvuutta koko joukosta tai emissioympäristöstä voidaan arvioida osajoukon sisältämän informaation näkökulmasta?
    - Millaisia menetelmiä on löydettävissä osajoukon tuottaman informaation arviointiin?
        - Miten emissiomalli määritellään?
        - Miten häiriöiden vaikutukset huomioidaan?
    - Millaisia mitallisia tuloksia menetelmillä on mahdollista tuottaa?
2) Miten osajoukolle määritellyt menetelmät ovat laajennettavissa koko joukon elektronisen aktiivisuuden arvioimiseksi?
3) Miten esitellyt menetelmät ovat hyödynnettävissä?
    - Millaisten elektronisen suojautumisen menetelmien arviointiin menetelmät soveltuvat?
    - Mitä etuja menetelmillä saavutetaan muihin arviointimenetelmiin verrattuna?
    - Mitä rajoitteita menetelmien käytössä on?

Pohjustuksena näihin varsinaisiin tutkimuskysymyksiin toimivat lyhyet kuvaukset elektronisen sodankäynnin määritelmistä, elektronisen suojautumisen menetelmistä sekä informaatioteorian käsitteet ja matemaattiset perusteet.

Loppuasetelmassa on päästy tilanteeseen, jossa tutkimuskysymyksiin on vastattu ja on arvioitu miltä osin menetelmien hyödyntäminen osana operatiivista suunnittelua tai operaatioanalyysia on sellaisenaan mahdollista ja miltä osin menetelmien hyödyntäminen edellyttää jatkotutkimuksia sekä kehittämistä.

1.3. Tutkimusmenetelmät ja rajaukset

Suunnittelua käytetään runsaasti tekniikan alan tutkimusmenetelmänä, koska lähtökohtaisesti tekniikan tehtävänä on uusien menetelmien ja laitteiden kehittäminen [41, s. 84]. Näin on myös tämän tutkimuksen kohdalla; tavoitteena on luoda menetelmiä, joilla voidaan vastata asetettuihin ongelmiin. Tekninen suunnittelu pyritään usein sitomaan viitemalliin, joka kuvaa ongelmanratkaisun yleisellä tasolla ja johon sitoen yksittäisongelmat voidaan elegantisti ratkaista [41, s. 85 - 86]. Tässä työssä viitemallin tapaisena pohjateoriana voidaan pitää informaatioteoreettisia määritelmiä, joihin sitoen tässä työssä esitetyt ongelmat on pyritty ratkaisemaan.

Matemaattiset tarkastelut esittävät varsin suurta roolia tavoitteena olevien menetelmien suunnittelussa. Matemaattisin menetelmin ei ole kuitenkaan suoranaisesti pyritty hakemaan yleispäteviä tuloksia tai sääntöjä koskien esimerkiksi elektronisen suojautumisen keinojen käyttöä ja tehoa. Lähestymistapa on siis teoreettinen ja painottaa elektronisen aktiivisuuden arvioinnissa hyödynnettävien menetelmien kehittämistä.

Käsittely pohjaa ennen kaikkea Shannonin [62] määritelmiin informaatiosta. Näin ollen informaatiota käsitellään sidottuna tilastollisiin todennäköisyysjakaumiin, joiden kautta informaation määrä on laskettavissa. Informaation semantiikkaan (merkitykseen, sisältöön) työssä ei suoranaisesti oteta kantaa (ks. esim. [5], [26] ja Weaverin artikkeli lähteessä [63]). Oletetaan siis, että esimerkiksi viestiliikenteen semanttinen sisältö ei ole tiedustelijan käytössä. Tämä onkin todennäköinen tulevaisuuden trendi, koska tiedonsiirtoliikenteen salaus tullaan ulottamaan yhä alemmille sotilasorganisaation tasoille [6, s. 86]. Perusolettamus on kuitenkin, että tiedustelija kykenee tunnistamaan erilaiset lähetteet ns. signaalien ulkoisten ominaisuuksien perusteella. Tällaisia ulkoisia ominaisuuksia ovat mm. taajuus ja erilaiset modulaatiot (ks. esim. [22, s. 112] ja [53, s. 3]). Tiedustelijan kannalta eroavaisuudet näissä ominaisuuksissa ovat ”teknistä semantiikkaa”, joita voidaan hyödyntää tilannekuvaa rakennettaessa.

Elektronisen aktiivisuuden tuottajina ja näin ollen elektronisen tiedustelun kohteina oletetaan olevan sotilasjoukon radio- ja millimetriaaltoalueella toimivat lähettimet. Voidaan siis sanoa, että rajoitutaan joukon tietoliikenne- ja tutkajärjestelmiin. Näin ollen esimerkiksi optisen alueen kohteita työssä ei käsitellä. Edettäessä vaiheeseen, jossa rakennetaan emissiomalleja osajoukolle ja joukolle, tarkastelu rajataan koskettelemaan vain tiedonsiirtojärjestelmiä. Syynä tähän on, että tutkajärjestelmien toiminnan kuvaaminen myöhemmin esiteltävien stokastisten prosessien avulla samaan tapaan kuin kuvataan viestijärjestelmien toimintaa, on varsin keinotekoista.

Käsiteltävää joukkoa ei sinänsä tarkasti rajata, vaikkakin käsittely ehkä parhaiten sopii maakomponentin taktisen tason joukoille. Joukon yksityiskohtaisia rakenteita, kalustoja tai kansallisuutta ei rajata millään tavalla.

Työssä tullaan esittelemään yhteensä neljä informaatioteoreettisiin määritelmiin pohjautuvaa menetelmää elektronisen aktiivisuuden arvioimiseksi. Kaksi ensimmäistä menetelmää mittaavat joukon tai osajoukon sisältämää informaatiota ja kaksi jälkimmäistä keskittyvät arvioimaan joukon tai osajoukon tuottaman informaation määrää. Menetelmät ovat toisistaan riippumattomia ja soveltuvat mittaamaan elektronista aktiivisuutta ja elektronisen suojautumisen tasoa vain yhdestä näkökulmasta. Nämä näkökulmat on tarkemmin esitelty luvussa 4.1. Työssä ei ole pyritty muodostamaan yhtenäismenetelmää, joka huomioisi kaikkien erillisten menetelmien näkökulman elektronista aktiivisuutta arvioitaessa. Yhtenäismenetelmää on lyhyesti sivuttu kartoitettaessa jatkotutkimustehtäviä (luku 6.4).

Menetelmien tuottamia tuloksia on havainnollistettu esimerkeillä, joita ei kuitenkaan ole sidottu mihinkään todellisiin joukkoihin. Menetelmien soveltaminen käytännön tilanteisiin on jätetty jatkotutkimusten tehtäväksi.

1.4. Aikaisempi tutkimus ja käytetyt lähteet

Työn perustuksen luo Shannonin klassinen teoria [62], [63], jonka määritelmiä ja tuloksia on laajasti hyödynnetty useilla eri aloilla. Tuota perustaa on täydennetty Rényin [55] johtamilla yleistyksillä, joilla informaation määrä kyetään laskemaan myös epätäydellisille todennäköisyysjakaumille. Oleellinen osa on myös Kullback:n ja Leiblerin määritelmillä [36], joiden avulla voidaan vertailla erilaisia todennäköisyysjakaumia.

Yllä mainittuja alkuperäisiä julkaisuja tukevaa kirjallisuutta ovat erityisesti [1], [4], [16], [37], [40] ja [56]. Näistä erityisesti [16] pidetään korkeatasoisena informaatioteoriaa ja sen sovelluksia läpileikkaavana teoksena, johon on useissa tutkimuksissa viitattu. Teoksen perusteella onkin havaittavissa, kuinka monelle eri osa-alueelle informaatioteoreettiset menetelmät ja tulokset ulottuvat. Näitä osa-alueita ovat mm.: tietoliikenneteoria, tietotekniikka, fysiikka, matematiikka, tilastotiede, todennäköisyyslaskenta ja taloustiede.

Lähempänä elektronisen sodankäynnin ongelmakenttää ovat erityisesti A. Bordenin esittelemät näkemykset ja käytännön sovellukset. Kuten mainittua, kimmoke tämän tutkimuksen näkökulmaan on saatu artikkelista [10][1], jossa korostetaan Shannonin teorian arvoa perustavanlaatuisena määritelmänä elektroniselle sodankäynnille ja informaatiosodankäynnille. Borden korostaa elektronisen sodankäynnin osalta Shannon – Hartley teoreeman merkitystä (ks. myös esim. [40, s. 187]). Tämä teoreema määrittelee tiedonsiirtoon soveltuvan kanavan maksimaalisen kapasiteetin seuraavasti

$$C = B\log_2\left(1+\frac{S}{N}\right), \qquad (1.1)$$

missä B = kanavan kaistanleveys

S/N = signaali-kohina suhde (kertoimena, ei dB).

Elektronisen suojautumisen menetelmillä pyritään turvaamaan mahdollisimman suuri kaistanleveys ja signaali-kohina suhde. Vastaavasti elektronisen vaikuttamisen menetelmillä pyritään vähentämään kanavan käyttömahdollisuuksia pienentämällä käytössä olevaa kaistanleveyttä ja signaali-kohina suhdetta. Edelleen Borden on korostanut yhtälössä 1.2[2] esitettyä määritelmää peruslausekkeena informaatiosodankäynnille:

$$I = H_{Ongelma} - H_{Jäljellä}, \qquad (1.2)$$

missä I = käyttöön saadun datan luoman informaation määrä

$H_{Ongelma}$ = ongelman alkuperäinen vaikeusaste

$H_{Jäljellä}$ = vaikeusaste, joka on jäljellä datan hyödyntämisen jälkeen.

[1] Vastaavat määritelmät on löydettävissä myös aikaisemmasta artikkelista [9].
[2] Määritelmä alun perin löydettävissä [40].

Yhtälö 1.2 perustuu vahvasti informaatioteoreettisiin määrittelyihin ja tämän typpistä lähestymistapaa tullaan käyttämään myös tässä tutkimuksessa. Tässä työssä käytettyä näkökulmaa korostaa kuitenkin enemmän seuraava määrittely:

$$I_{Tilannekuva} = H_{Todellisuus} - H_{Häiriötekijät}. \qquad (1.3)$$

Toisin sanoen, erilaiset häiriötekijät, kuten elektronisen suojautumisen menetelmät, estävät tiedustelijaa saavuttamasta tilannekuvaa, joka täydellisesti vastaisi todellisuutta (olettaen, että $H_{Häiriötekijät} \neq 0$).

Borden on esitellyt myös sovellutuksia ([7], [8], [20], [10] [11]), jotka hyödyntävät informaatioteoreettisia ja todennäköisyyslaskentaan perustuvia menetelmiä. Nämä sovellukset liittyvät päätöksentekojärjestelmiin eivätkä sinänsä koskettele elektronisen aktiivisuuden ja elektronisen suojautumisen arviointia. Myöskään muita tästä näkökulmasta tehtyjä informaatioteoriaan pohjautuvia tutkimuksia ei ole ollut tutkijan tiedossa. Toisaalta on huomattava, että informaatioteoreettista tutkimusta on tehty eri maissa huomattavia määriä. Kaikki nämä tutkimukset eivät välttämättä ole tämän työn tekijän saatavilla.

Elektronisia järjestelmiä ja elektronista sodankäyntiä koskketteleva lähdemateriaali sisältää kohtuullisen laajan otoksen alaan liittyvää kirjallisuutta ja artikkeleita. Kirjallisuuden ikähaarukka asettuu välille 1966 – 2009 painopisteen ollessa 2000-luvun vaihteessa ja edelleen 2000-luvun puolella. Viimeisintä tietoa olemassa olevista elektronisen sodankäynnin järjestelmistä on haettu eri laitevalmistajien internet sivuilta, joilta löytyy järjestelmiin liittyvää esittelymateriaalia.

1.5. Tutkimusraportin rakenne

Tutkimusraportin luvut 2 ja 3 johdattelevat lukijan sähkömagneettisen toimintaympäristön ja informaatioteorian peruskäsitteisiin. Luvun 2 painopiste on elektronisen sodankäynnin osa-alueiden kuvaamisessa. Luvussa 3 esitellään informaatioteoreettiset peruskäsitteet ja myöhemmin sovellettavat matemaattiset perusteet.

Luku 4 on työn pääluku ja siinä johdetaan teoreettisen perusteiden pohjalta menetelmät, joita hyödyntämällä voidaan arvioida osajoukon elektronista aktiivisuutta ja elektronisen suojautumisen menetelmien vaikuttavuutta eri olosuhteissa. Luvussa 4 haetaan vastausta 1. tutkimus-

kysymykseen. Luvussa 5 kehitetyt menetelmät laajennetaan koskettamaan soveltuvilta osin koko joukkoa. Lisäksi lukuun 5 on sisällytetty arviointi kehitettyjen menetelmien hyödynnettävyydestä. Luvussa 5 haetaan vastauksia tutkimuskysymyksiin 2 ja 3. Yhteenveto tutkimustuloksista ja johtopäätökset esitellään luvussa 6.

Työhön on liitetty varsin paljon esimerkkejä, joilla pyritään havainnollistamaan esiteltyjen menetelmien tuottamia tuloksia ja niiden hyödynnettävyyttä. Tämä luo tutkimusraportille hieman oppikirjamaisia piirteitä. Esimerkkien runsaus on katsottu tarpeelliseksi etenkin, koska vastaavaa näkökulmaa käsiteltyyn aiheeseen ei ainakaan yleisesti ole ollut saatavilla.

Laskennallisesti laajat matemaattiset todistukset ja esimerkkien yksityiskohtaiset laskutoimitukset on sijoitettu liitteisiin.

2. SÄHKÖMAGNEETTINEN TOIMINTAYMPÄRISTÖ

2.1. Yleistä

Sotilaallisesta näkökulmasta katsottuna sähkömagneettisen toimintaympäristön muodostavat sähkömagneettista spektriä hyödyntävät omat ja vihollisen joukot sekä järjestelmät. Oleellisena osana sähkömagneettista toimintaympäristöä ovat nykyaikana myös muut valtiolliset ja kaupalliset toimijat sekä näiden hyödyntämät tai valmistamat järjestelmät. Kaikki nämä toimijat tuottavat aktiivisuutta sähkömagneettiseen spektriin ja tällä saattaa olla vaikutuksia erilaisten tietoliikenne- ja sensorijärjestelmien käytettävyydelle. Tätä kokonaisnäkökulmaa ei tässä työssä tarkemmin käsitellä, vaan painopisteenä on yksittäisen joukon elektronisen aktiivisuuden ja elektronisten suojautumismenetelmien arvioinnissa.

Elektronisen aktiivisuuden ja elektronisen suojautumisen arvioinnin kannalta on oleellista tuntea elektronisen sodankäynnin yleiset käsitteet toteuttamisperiaatteet. Perusteet on esitelty tässä luvussa painopisteen ollessa elektronisessa tuessa ja elektronisessa suojautumisessa. Tarkasteltavien joukkojen organisaatioista, varustuksesta ja käyttöperiaatteista ei esitellä mitään hahmotelmia, koska lähtökohtaisesti joukon ominaisuuksia ei ole millään tavalla rajattu. Näillä seikoilla ei ole myöskään tämän työn jatkokäsittelyjen kannalta merkitystä.

2.2. Elektronisen sodankäynnin perusteet

2.2.1. Elektronisen sodankäynnin osa-alueet

Elektroninen sodankäynti jaetaan tyypillisesti kolmeen osa-alueeseen, jotka ovat:

- Elektroninen tuki (ELTU, Electronic Support, ES)
- Elektroninen vaikuttaminen (ELVA, Electronic Attack, EA)
- Elektroninen suojautuminen (ELSU, Electronic Protection, EP) [29] ja [34].

Elektronisella tuella kerätään tietoa ympäristössä esiintyvistä sähkömagneettista säteilyä lähettävistä laitteista. Tavoitteena on muodostaa elektroninen maalitilannekuva, jolla voidaan tukea eri johtoportaiden päätöksentekoa tai tarjota välitön uhkavaroitus jollekin alustalle tai joukolle [34]. Suomalaisen jaottelun mukaisesti elektronisen tuen järjestelmät ja joukot palvelevat ennen muuta operatiivis-taktisen tasan (sotanäyttämö) johtoportaita [34]. Signaalitiedustelu

(Signal Intelligence, SIGINT) kategorisoidaan strategisen tasan (valtakunnallinen) toiminnaksi, jonka tavoitteena on pitkäjänteinen kohteiden seuranta siten, että perusta strategiselle ennakkovaroitukselle kyetään luomaan [30, s. 50 ja 90]. Tässä työssä ei sinänsä erotella millä tasalla tai minkä määrittelyn mukaisesti tiedustelija toimii, vaan elektronisen tuen (ELTU) käsitettä käytetään yleisnimityksenä elektroniselle tiedustelutoiminnalle. Varsin usein käytetään myös yleisnimikettä tiedustelujärjestelmä. Luvussa 2.2.2 on käsitelty elektronista tukea hieman syvällisemmin.

Elektronisella vaikuttamisella pyritään häiritsemään, lamauttamaan tai tuhoamaan vastustajan sähkömagneettista spektriä käyttävät tai muut elektroniikasta riippuvat järjestelmät. Käytettyjä keinoja ovat muun muassa viestiyhteyksien ja sensorijärjestelmien elektroninen häirintä, laitteiden vahingoittaminen tai tuhoaminen suunnatun energian aseilla (esim. HPM, High Power Microwave) sekä fyysinen tuhoaminen esimerkiksi säteilyyn hakeutuvilla asejärjestelmillä [34]. Tässä työssä elektronista vaikuttamista ei jatkossa käsitellä.

Elektronisen suojautumisen tavoitteena on varmistaa omien elektronisten järjestelmien käytettävyys tahallisten tai tahattomien vaikutusten alaisena (esim. häirintä tai asejärjestelmiltä suojautuminen) sekä vaikeuttamaan vastustajan tiedustelutoimintaa [34]. Elektronista suojautumista on käsitelty tarkemmin luvussa 2.2.3.

2.2.2. Elektroninen tuki

Elektronisen tuen tärkeimpiä kohteita ovat erilaiset langattomat tiedonsiirtojärjestelmät ja muut sähkömagneettista säteilyä lähettävät laitteet kuten tutkat. Tyypillisesti elektroninen tuki jaetaankin viestitiedusteluun (COMINT, communication intelligence) ja elektroniseen mittaustiedusteluun (ELINT, electronic intelligence)[3]. Elektronisen tuen päämääränä on havaita, tunnistaa, paikantaa ja analysoida ympäristössä esiintyvät sähkömagneettista säteilyä lähettävät lähettimet [61]. Signaalin havaitsemiseen liittyvät käsitteet ja problematiikkaa on esitelty luvussa 4.3.3. Muihin päämääriin liittyviä tekijöitä on esitelty alla niiltä osin, kuin näillä on merkitystä tämän työn kannalta.

Tunnistaminen perustuu manuaaliseen tai automaattiseen signaalin analysointiin, jonka perusteella lähettimen tyyppi ja mahdollisesti myös lähettimen sisältävä lavetti sekä joissain tapa-

[3] COMINT ja ELINT liitetään yleensä käsitteen SIGINT alalajeiksi. Joissain lähteissä myös esimerkiksi tietoverkkotiedustelu (e-SIGINT) ja vieraiden laitteiden tiedustelu (FISINT) liitetään signaalitiedustelun alalajeiksi [30, s. 50].

uksissa jopa lähetintä käytävä joukko voidaan tunnistaa. Lähettimen tai lähetteen tunnistaminen perustuu lähetetylle signaalille tyypillisiin elektronisiin parametreihin [53] ja [71], joita voivat viestisignaalien osalta olla esimerkiksi [53, s. 304 - 305]:

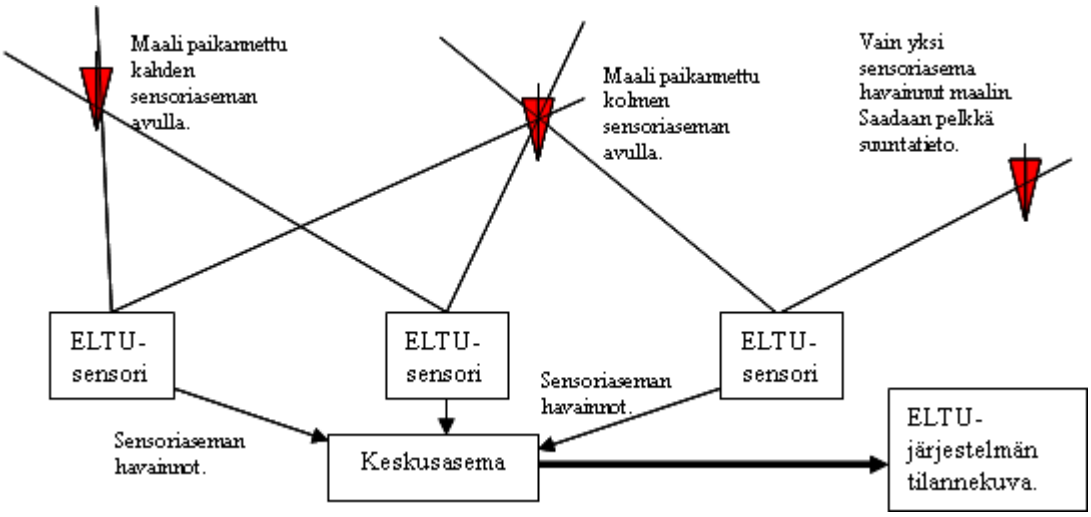
- modulaatio (esim. AM, FM tai PM)
- signaalin tyyppi (esim. analoginen tai digitaalinen)
- digitaalisen signaalin kyseessä ollessa modulaatio (esim. FSK, PSK jne.)
- kanavoidun signaalin kyseessä ollessa kanavoinnin tyyppi (esim. FDMA, TDMA.. jne
- lähettimen taajuus/taajuusalue.

Tutkasignaalien osalta tyypillisiä tunnistuksessa käytettäviä parametreja ovat [71, s. 272]:

- taajuus
- pulssintoistoväli
- pulssintoistomodulaatio
- pulssinpituus
- antennin keilaustapa ja –aika.

Joissain tapauksissa voidaan lähetin tai lähetintä käyttävä henkilö tunnistaa tietyksi yksilöksi (identifioida). Tämä on mahdollista, jos laitteessa on jokin yksilöllinen anomalia verrattuna muihin samanlaisiin laitteisiin tai esimerkiksi henkilön äänen tai sähkötystyylin perusteella [22, s. 58] [53, s. 324 - 329].

Lähettimen paikantaminen perustuu kahden tai useamman ELTU-sensorin tekemiin suunta- tai aikaeromittauksiin [52]. Tyypillisesti yksittäisten sensoriasemien tekemät havainnot yhdistetään tilannekuvaksi ns. keskusasemalla. ELTU-järjestelmän toimintaperiaate on esitetty kuvassa 2.1.



Kuva 2.1: Useasta ELTU-sensoriasemasta koostuvan ELTU-järjestelmän toimintaperiaate. Vrt. esim. [48, s. 297].

Elektronisella tuella kerätyn materiaalin pohjalta voidaan tehdä monenlaisia teknisiä ja taktis-operatiivisia analyyseja. Taktis-operatiivisessa analyysissa tehdään tiedustelutietojen pohjalta johtopäätöksiä esimerkiksi laitteiden ja joukkojen ryhmityksistä, määrästä, komentopaikkojen sijainnista sekä nykyisestä ja tulevasta toiminnasta [22, s. 135]. Seuraavassa kappaleessa on kuvattu viestiliikenteeseen perustuvan analyysin perusteita pohjautuen lähteeseen [22, s. 135 - 138].

Tiedustelun kohteena olevasta joukosta voidaan tehdä päätelmiä seuraamalla viestiliikenteen määrää ja suuntautumista. Tyypillisesti erilaisiin kenttäradioverkkoihin voidaan liittää hierarkkinen liikennöintikulttuuri, jossa joukon johtaja/komentopaikka liikennöi kaikkien alaistensa ja ylemmän johtoportaan kanssa. Varsin usein tällainen johtoasema erottuu selkeästi alaasemistaan huomattavasti suuremman viestiliikenteen määrän johdosta. Vastaavasti jonkin joukon viestiliikennetarpeita varten muodostetun taktisen runkoverkon tukiasemat on mahdollista erottaa liikennemäärän perusteella. Jotta liikennemääriin perustuva analyysi olisi tehokasta, tulee lähetteet kyetä myös paikantamaan (suuntimaan). Kenttäradioverkkoihin liittyy tyypillisesti ominaisuus, jossa samaan verkkoon kuuluvat asemat käyttävät samaa taajuutta. Tämän kiinteän taajuuden perusteella tiedustelija pystyy varsin usein päättelemään verkkoon kuuluvat asemat. Hyppivätaajuisten radioiden käyttö saattaa vaikeuttaa tämän tyyppistä päättelyä. Mikäli asemat kyetään myös paikantamaan, paljastuu verkon rakenne ja tätä kautta mahdollisesti sen käyttötarkoitus ja edelleen käyttävä joukko. Salaamaton viestiliikenne saattaa tarjota tiedustelijalle erittäin monipuolista tietoa alkaen erilaisista asemakutsuista joukon toiminnan ja suunnitelmien kuvaamiseen saakka. Edellä kuvattu hierarkkinen verkkorakenne ei ole kuitenkaan itsestäänselvyys, vaan erilaisilla elektronisen suojautumisen keinoilla ja tiedon jakeluun liittyvillä tekniikoilla voidaan vaikeuttaa johtosuhteiden erottumista.

2.2.3. Elektroninen suojautuminen

Elektronisen suojautumisen aktiivisilla ja passiivisilla[4] menetelmillä suojataan omien elektronisten järjestelmien suorituskyky tahattomilta häiriöiltä ja vastustajan tahalliselta vaikuttamiselta sekä asejärjestelmiltä [29] ja [34]. Lisäksi elektronisen suojautumisen alle liitetään toimenpiteitä, joilla vaikeutetaan elektronista tukea [34]. Taulukkoon 2.1 on koottu suojautumismenetelmiä, joilla voidaan vaikeuttaa elektronisen tuen tuloksellista toteuttamista. Mene-

[4] Aktiivisen suojautumisen menetelmät ovat vastustajan havaittavissa ja ovat näin ollen tyypillisesti teknisiä. Passiiviset menetelmät eivät ole sellaisenaan vastustajan havaittavissa ja ovat tyypillisesti toiminnallisia ja taktisia. [6, s. 55]

telmäluettelo on yhteenveto kirjallisuudessa [6, s. 55 - 86], [30, s. 94 - 95] ja [33, s. 26 - 28] esitellyistä keinoista.

Menetelmä ja kuvaus	Tekninen/ Toiminnallinen/ Taktinen	Aktiivinen/ Passiivinen
LPI (Low Probability to Intercept) ja LPD (Low Porbability to Detec) tekniikat Menetelmillä pyritään vaikeuttamaan signaalin sieppaamista ja ilmaisua. Esimerkkeinä taajuus hypytys ja suorasekvenssitekniikat.	Tekninen	Aktiivinen
Viestiliikenteen salaaminen - Datan tekninen salaaminen salausalgoritmeilla - Viestiliikennekuri ml. peitteistöjen käyttö	Tekninen Toiminnallinen	Aktiivinen
Toimintaparametrien säätely Esimerkiksi lähetystehojen optimointi, modulointitavat ja lähetteiden polarisaatiot sekä niiden muutokset.	Tekninen Toiminnallinen	Aktiivinen
Maskaus Elektronisen tiedustelujärjestelmän aktiivinen häirintä siten, että omia hyötylähetteitä ei kyetä havaitsemaan.	Tekninen Toiminnallinen	Aktiivinen
Laitteistojen ja lähetteiden identtisyys Erilaisten joukkojen varustaminen identtisellä kalustolla vaikeuttaa tiedustelijan johtopäätösten tekoa. Yksittäiseen tai muutamaan lähettimeen liittyvien anomalioiden poistaminen vaikeuttaa näiden laiteyksilöiden seuraamista. Edellyttää toimia kaikilla tasoilla.	Toiminnallinen Taktinen Tekninen	Passiivinen
Maaston hyväksikäyttö Esimerkiksi tiedustelun vaikeuttaminen maastoesteitä hyödyntämällä. Toiminnallinen menetelmä käsiteltäessä yksittäisen laitteen käyttöperiaatteita. Taktinen menetelmä otettaessa huomioon sotilasjoukon operaatiossa.	Toiminnallinen Taktinen	Passiivinen
Suunta-antennit Suuntaamalla teho kapealle sektorille on mahdollista vaikeuttaa signaalin havaitsemista olettaen, että tiedustelusensori ei sijaitse pääkeilan suunnassa. Voidaan mieltää myös taktisen tasan menetelmäksi, mikäli huomioidaan esim. sotilasjoukon viestisuunnitelmien teossa.	Toiminnallinen Taktinen	Passiivinen
Liike Joukkojen ja järjestelmien liikkeellä hidastetaan tiedustelutoimintaa, koska tiedustelija joutuu uhraamaan yhä uudestaan resursseja saman asian analysoimiseksi.	Toiminnallinen Taktinen	Passiivinen
Emissioiden hallinta (EMCON, Emission Control) Säätelemällä joukkojen ja järjestelmien emissioita ajallisesti, alueellisesti ja toimintaan liittyen pyritään estämään tai vaikeuttamaan tiedustelijan työtä. Emissioiden hallintaan oletetaan kuuluvan myös taajuushallinnan ja laitteiden tahattomasti vuotavan säteilyn hallinnan.	Toiminnallinen Taktinen	Passiivinen
Harhauttaminen Harhauttavilla toimilla annetaan väärä kuva esim. omasta ryhmityksestä ja toiminnasta. Tällä vaikeutetaan oikean tilannekuvan muodostamista. Joskus tämän tyyppinen harhauttaminen asetetaan elektronisen vaikuttamisen alaisuuteen. Tässä sitä käsitellään kuitenkin elektronisen suojautumisen elementtinä.	Taktinen Toiminnallinen	Aktiivinen Passiivinen

Taulukko 2.1: Elektronista tukea vaikeuttavia elektronisen suojautumisen menetelmiä.

Elektronisen suojautumisen toimenpiteet voidaan jakaa teknisiin, toiminnallisiin ja taktisiin [6, s. 56] ja [33, s. 27]. Teknisillä menetelmillä ymmärretään laitteistojen ja järjestelmien omi-

naisuudet, joita voidaan hyödyntää elektroniselta tiedustelulta suojautumisessa. Toiminnallisilla menetelmillä ymmärretään laitteiden ja järjestelmien käyttöperiaatteita sekä elektronisen suojautumisen huomioivaa ohjeistusta ja toimintakulttuuria. Taktisen tasan menetelmät mielletään sotilasjoukon taktiseen tai operaatiotaidolliseen käyttöön liittyviksi toimenpiteiksi.

2.2.4. Emissioiden hallinta (EMCON)

Emissioiden hallinta (emissiokontrolli) on tärkein työkalu elektroniselta tuelta suojauduttaessa [34]. Esimerkkinä mainittakoon Yhdysvaltain taktisen tasan elektronisen tuen tehottomuus valmistauduttaessa maahyökkäykseen Irakissa 1991. Irakilaiset joukot kommunikoivat pääsääntöisesti kaapeliyhteyksiä hyödyntäen, joten elektronisen tuen tulokset olivat varsin mitättömiä [64]. Tässä luvussa esitellään muutamia määritelmiä ja näkemyksiä emissioiden hallinnasta toiminnallisena ja taktisena suojautumismenetelmänä.

Suomalaisessa ELSO-alan kirjallisuudessa [33], [34] emissiokontrolli mielletään omien lähetteiden hallinnaksi siten, että järjestelmien toiminnalliset ja tahattomat sähkömagneettiset emissiot tunnetaan ja minimoidaan. Tavoitteena on, että minimoidaan vastustajan mahdollisuudet havaita, analysoida, luokitella, tunnistaa, yksilöidä ja paikantaa omia järjestelmiä sekä estää näitä vastaan kohdistuvien vastatoimien optimointi. Emissioiden hallintaa tukee taajuushallinta, jonka tarkoituksena on omien järjestelmien ja joukkojen käyttämien taajuuksien allokointi siten, että päällekkäisyydet, häiriöt ja luvattomien taajuusalueiden käyttö saadaan eliminoitua. Suomalaisen jaottelun mukaisesti taajuushallinta ei ole osa elektronista sodankäyntiä [30, s. 97], vaan johtamisjärjestelmäalan hallinnoimaa toimintaa.

Länsimaiset määritelmät (ks. esim. [12] tai [29]) emissioiden hallinnalle ovat varsin yhteneväiset yllä esitetyn kanssa. On kuitenkin huomionarvoista, että länsimaisessa ajattelussa taajuushallinta mielletään osaksi elektronisen sodankäynnin kokonaisuutta. Yhdysvaltalaisissa standardeissa [17] määritellään myös vaatimukset elektronisten laitteiden tahattomille emissioille; max -105 dBm/m^2 kilometrin päässä laitteesta taajuusalueella 500 kHz – 40 GHz.

Emittoitavan sähkömagneettisen säteilyn määrää voidaan vähentää rajoittamalla kaikkien tai joidenkin elektronisten laitteiden käytön tasoa. Tyypillisiä esimerkkejä ovat radiohiljaisuus, jonka vallitessa radioiden käyttö on kiellettyä ja elektroninen hiljaisuus, joka rajoittaa kaikkien elektronisten laitteiden käyttöä [6, s. 57].

Jotkin näkemykset [65] korostavat emissioiden hallinnan kokonaisvaltaisuutta. Tolvanen *et al.* ovat korostaneet, että emissioiden hallinta on ennen muuta emissioiden käytön suunnittelua siten, että omia ase-, johtamis-, paikannus- ja ELSO-järjestelmiä kyetään käyttämään parhaalla mahdollisella tavalla joukon taktisen tehtävän toteuttamiseksi. Näin ollen emissiokontrolli ei ole vain omien lähetteiden rajoittamista erilaisten EMCON-tasojen muodossa, vaan yhtä hyvin emissioiden käytön optimointia tehtävän mukaisesti.

Emissioiden hallinta mielletään tyypillisesti koskevan radio- ja mikroaaltoalueiden taajuuksia, joilla tiedonsiirto- ja sensorijärjestelmät toimivat. Joidenkin näkemysten [35] mukaisesti emissioiden hallinta voidaan laajentaa käsittämään myös muunlaisia herätteitä, jotka voivat ilmaista kohteen olemassaolon. Tällaiset herätteet voivat perustua mm. lämpöön, magneettisuuteen, ääneen ja seismisyyteen. Tässä työssä ei käsitellä tämän tyyppisiä herätteitä.

3. MATEMAATTISET PERUSTEET

3.1. Yleistä

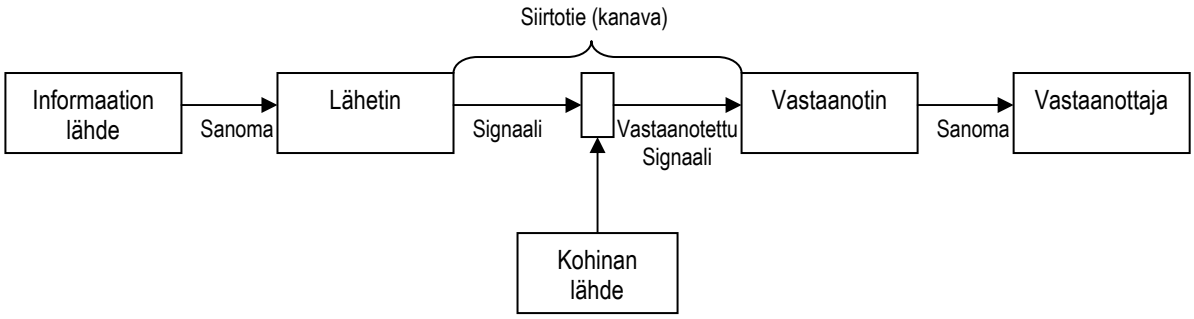
Eräs informaatioteorian perustavaa laatua oleva tavoite on määrittää mitta informaation määrälle. Näitä mittareita ja niistä johdettuja sovelluksia on hyödynnetty monella eri tieteenalalla viimeisen 60 vuoden kuluessa (ks. esim. [16]). Informaatioteorian tärkeimpiä käsitteitä ovat entropia, yhtenäisinformaatio ja suhteellinen entropia. Myös tässä työssä tullaan soveltamaan näitä määritelmiä rakennettaessa menetelmiä elektronisen aktiivisuuden ja elektronisen suojautumisen tason mitalliseksi arvioimiseksi. Informaation yhteenlaskettavuudella on myös merkittävä rooli jatkokäsittelyn kannalta ja tämän ominaisuuden perusteita onkin melko tarkasti kuvattu luvussa 3.2.2. Emissioympäristön mallintaminen edellyttää ns. stokastisten prosessien hyödyntämistä.

Luvussa 3.2 esitellään informaatioteorian peruskäsitteet ja niiden matemaattiset perusteet. Luvut 3.2.1, 3.2.2, 3.2.3, 3.2.4 ja 3.2.5 ovat lähes kokonaisuudessaan teoksiin [62] ja [63] perustuvia. Viittaukset muihin yksittäisiin lähteisiin on esitetty tekstissä. Stokastisia prosesseja sivutaan jo luvussa 3.2.3, mutta perusteellisempi käsittely toteutetaan vasta luvussa 3.3.

3.2. Informaatioteorian perusteet

3.2.1. Informaatiota siirtävä järjestelmä

Shannon on kuvannut informaatiota välittävän järjestelmän ja siihen sisältyvät elementit kuvan 3.1 mukaisesti [62]. Lähtökohtaisesti esitetty järjestelmä on helppo mieltää koskettelevan sähköistä tiedonsiirtoa; esimerkiksi tekstiviestin lähettämistä henkilöltä A henkilölle B. Kuten Weaver on tekstissään [63] kuvannut, on Shannonin teoria kuitenkin miellettävä laajemmassa mittakaavassa, kosketellen missä tahansa muodossa olevan informaation siirtämistä tiedon lähteeltä vastaanottajalle. Seuraavassa on lyhyesti kuvattu informaatiota siirtävän järjestelmän elementtien määrittelyt [62] ja [63] mukaillen.



Kuva 3.1: Yleiskuvaus informaatiota siirtävästä järjestelmästä [62, s. 2].

Informaation lähde tuottaa sanoman tai jakson sanomia, jotka on määrä siirtää vastaanottajalle. Informaation lähteenä toimii hyvin usein ihminen, mutta lähde voi olla myös esimerkiksi ympäröivä luonto ja sen ilmiöt. Periaatteessa sanoma voi olla miten tahansa muodostettu, esimerkiksi: a) Kirjaimista (merkeistä/symboleista) muodostettu jakso (esim. lause). b) Ajan funktiona muodostettu (jatkuva) muuttuja (esim. puhe, analoginen tv-kuva, musiikki). c) Fyysisesti paperille kirjattu teksti tai kuva.

Lähetin koodaa muodostetun sanoman siten, että se sopii lähetettäväksi siirtotiellä (muodostetaan lähetettävä signaali). Esimerkiksi matkapuhelin koodaa tekstiviestisanoman sopivalla tavalla siten, että signaali sopii lähetettäväksi siirtotiellä, jona toimii ympäröivä avaruus ja jossa signaali etenee sähkömagneettisena säteilynä. Lähettimenä voi toimia myös vaikkapa puhekyky, jolle aivot ovat tuottaneet lähetettäväksi tarkoitetun sanoman. Aivojen tuotos koodataan puheeksi ja lähettää kanavalle (ilma).

Siirtotiellä signaaliin vaikuttaa kohina, joka vaimentaa tai vääristää signaalia. Kohinan lähteenä voi olla ympäröivän luonnon ilmiöt tai kohina voi olla ihmisen toiminnasta johtuvaa. On myös huomattava, että osa signaaliin vaikuttavasta kohinasta voi olla peräisin lähettimestä ja/tai vastaanottimesta. Kuvassa 3.1 kaikki kohinan aiheuttajat on yhdistetty yhdeksi lähteeksi.

Yleensä vastaanotin muodostaa uudelleen (dekoodaa) lähteen aikoman sanoman suorittamalla käänteiset toimenpiteet lähettimeen verrattuna. Esimerkiksi tekstiviestin vastaanottava matkapuhelin purkaa signaalin koodauksen ja esittää sanoman päätelaitteella. Vastaavasti kuuloaisti vastaanottaa puheen.

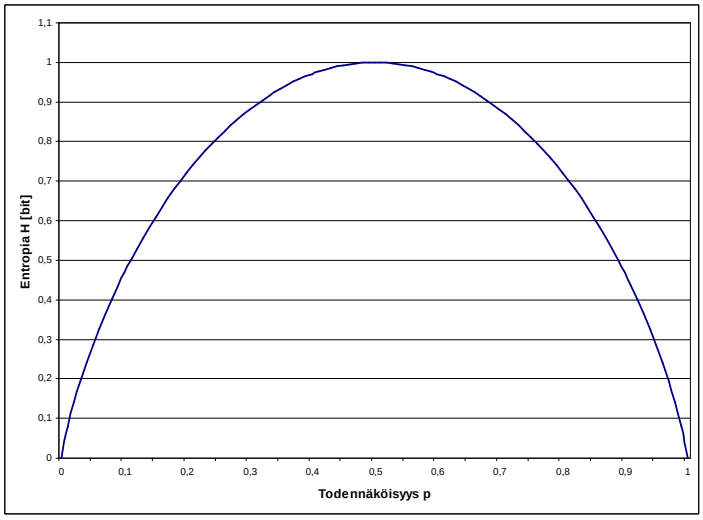
Vastaanottaja on varsin usein ihminen, mutta se voi olla myös esimerkiksi tietojärjestelmä tai vaikkapa kotieläin.

3.2.2. Informaatio ja entropia

Käsitteellä informaatio ei tässä yhteydessä käytetä merkityksessä, joka on tyypillinen arkikielelle. Yleensä informaatioon liitetään jokin merkitys; mikäli lukija ei ymmärrä jotain tekstiä, sillä ei ole mitään merkittävyyttä lukijalle eikä teksti näin ollen ole informatiivinen. Shannonin teoreeman näkökanta informaatioon ohittaa merkityksen. Näin ollen esimerkiksi mitkä tahansa samanmittaiset kirjainyhdistelmät sisältävät yhtä paljon informaatiota riippumatta siitä, missä järjestyksessä yhdistelmän kirjaimet ovat. Shannonin teoreeman (ks. [62, s. 10 - 11]) mukaisesti informaatiolla tarkoitetaan valinnan vapautta; mitä enemmän informaatiota, sitä enemmän vaihtoehtoja tehdä valinta. Informaation määrän mittarina käytetään entropiaa. Esimerkiksi jonkin järjestelmän entropian kasvaessa lisääntyy epävarmuus. Toisin sanoen valittavien vaihtoehtojen määrän kasvaessa on entistä vaikeampaa päätellä, mikä vaihtoehto seuraavaksi toteutuu. Voidaan myös ajatella, että informaation lisääntyessä on koko ajan vaikeampi sattumalta osua oikeaan vaihtoehtoon (olettaen, että tilanteessa on vain yksi ”oikea” vaihtoehto). Jos oletetaan, että tilanteessa on n kappaletta vaihtoehtoja ja eri vaihtoehtojen todennäköisyydet ovat $p_1, p_2, \ldots, p_n$, niin tällöin entropia[5] määritellään yhtälöllä

$$H = -\sum_{i=1}^{n} p_i \log p_i \,. \qquad (3.1)$$

Mikäli logaritmissa käytetään kantalukuna numeroa kaksi, voidaan entropian yksikkönä käyttää termiä bitti. Tässä työssä logaritmifunktion kantalukuna on aina kaksi. Muunnos luonnollisesta logaritmista kaksikantaiseen voidaan tehdä yhtälön 3.2 avulla. Kuvassa 3.2 on esitetty entropia tilanteessa, jossa on kaksi vaihtoehtoa todennäköisyyksien ollessa p ja $q = 1 - p$.



Kuva 3.2: Entropia todennäköisyyden p funktiona [62, s. 11].

[5] Tästä määrittelystä käytetään monesti nimitystä Shannonin entropia. Jatkossa on syytä huomata, että $-\sum p \log p = \sum p \log \frac{1}{p}$.

$$\log_2 x = \frac{\log_e x}{\log_e 2} = \frac{\ln x}{\ln 2} \approx 1.44 \ln x \qquad (3.2)$$

Entropialla on useita ominaisuuksia, jotka on tarkemmin esitelty lähdekirjallisuudessa (ks. esim. [1], [16], [62] ja [63]). Tämän työn kannalta oleellisimpia ominaisuuksia ovat seuraavat:

1. $H = 0$ vain ja vain jos kaikkien vaihtoehtojen paitsi yhden todennäköisyys on nolla. Tämän mainitun vaihtoehdon todennäköisyys on yksi eli tilanteessa ei ole mahdollisuutta valita eri vaihtoehtojen välillä.
2. Entropia on suurin silloin, kun kaikkien vaihtoehtojen todennäköisyydet ovat yhtä suuret. Jos vaihtoehtoja on n kappaletta, on entropia tällöin $H = \log(n)$.
3. Kaksi toisistaan riippumatonta tapahtumaa tuottavat informaatiomäärän, joka vastaa yksittäisten tapahtumien entropioiden summaa, eli $H(pq) = H(p) + H(q)$ [1, s. 3].

Ominaisuus numero kolme yllä tarkoittaa toisistaan riippumattomien entropioiden yhteenlaskettavuutta, joka on perusolettamus lähes kaikille aksiomaattisille järjestelmille, joilla kuvataan informaation olemusta (ks. esim. [1, s. 3 ja 30 - 31], [37, s. 12 - 13] ja [56, s. 542 ja 553]). Tämä olettamus täyttyy erityisesti logaritmisissa määrittelyissä, koska $\log(pq) = \log p + \log q$. Yleisemmin voidaan mieltää seuraavasti: jos A ja B ovat esimerkiksi toisistaan riippumattomia kokeiluja, joihin sisältyviä tapahtumia vastaavat diskreetit todennäköisyysjakaumat $P = (p_1, \ldots, p_m)$ ja $Q = (q_1, \ldots, q_n)$, niin tällöin kokeiden A ja B samanaikainen toteuttaminen tarkoittaa kokeilun AB tekemistä ja nyt jokaista yhteistä tapahtumaa vastaa todennäköisyys $p_i q_j$ ($i = 1, 2, \ldots, m$ ja $j = 1, 2, \ldots, n$) [56, s. 553]. Jakauma $P * Q = \{p_i q_j\}$ on toisistaan riippumattomien jakaumien P ja Q suora tulo ja nyt pätee seuraava määrittely entropioiden yhteenlaskettavuudelle [56, s. 553]:

$$H(P * Q) = H(P) + H(Q). \qquad (3.3)$$

Yksityiskohtaisemmin kirjattuna yhtälö 3.3 saadaan muotoon [1, s. 30]

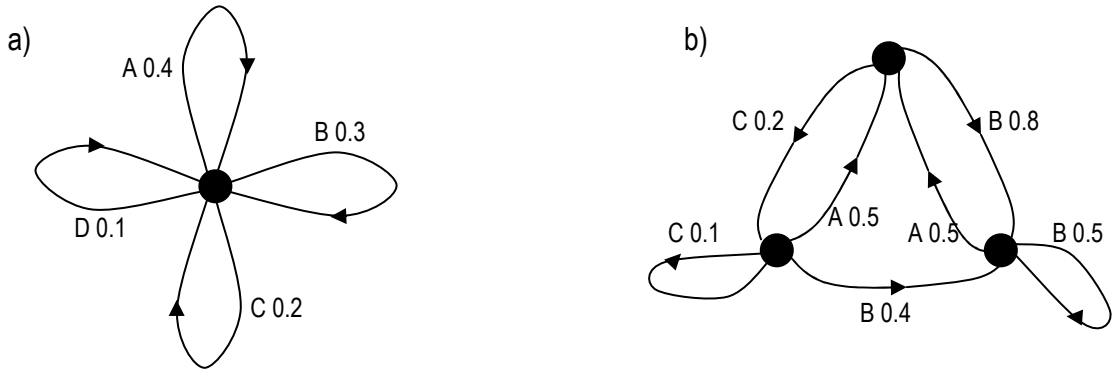
$$H(p_1 q_1, p_1 q_2, \ldots, p_1 q_n, p_2 q_1, \ldots, p_2 q_n, \ldots, p_m q_1, \ldots p_m q_n) = H(p_1, p_2, \ldots, p_m) + H(q_1, q_2, \ldots, q_n). \qquad (3.4)$$

Kuten edellä on kerrottu, entropia on lähtökohtaisesti epävarmuuden mittayksikkö. Entropia voidaan kuitenkin mieltää myös jonkin tilastollisen järjestelmän tai kokeen tuottamaksi, mah-

dollisesti hyödynnettävissä olevaksi, informaation määräksi [55]. Eli periaatteessa epävarmuus jonkin kokeilun lopputuloksesta ennen kokeen suorittamista on sama, kuin informaation määrän, joka odotetaan saatavan käyttöön kokeen toteuttamisen jälkeen [1, s. 29].

3.2.3. Diskreetti informaation lähde

Diskreetissä järjestelmässä informaation lähde tuottaa kanavalle jaksoja (sanoja, lauseita, sanomia), jotka koostuvat yksittäisistä symboleista. Käytössä olevien symboleiden lukumäärän tulee olla äärellinen. Jaksojen muodostumista voidaan säädellä asettamalla kullekin symbolille todennäköisyys, jolla se tulee valituksi. Jos jaksoista on tarpeen muodostua esimerkiksi ymmärrettäviä sanoja, ei peräkkäisiä symboleita tyypillisesti voida valita mielivaltaisesti. Esimerkiksi kirjainyhdistelmän QÖ esiintyminen suomenkielisessä sanassa on hyvin epätodennäköistä. Mikäli peräkkäisten symbolien valintaa on jotenkin rajoitettu, on informaation lähteellä tällöin useita erilaisia ”tiloja”, jotka kaikki voivat toimi symboleiden tuottajina. Jos peräkkäisten symboleiden valintaa säädellään vain kullekin symbolille ominaisella todennäköisyydellä, niin tällöin informaation lähde omaa vain yhden ”tilan”. Kuvassa 3.3 on selvennetty näiden kahden tapauksen eroa.



Kuva 3.3: a) Informaation lähde, jossa peräkkäisten symbolien valinta toisistaan riippumaton toimenpide. Prosessissa vain yksi tila. b) Lähde, jossa peräkkäisten symbolien valinta riippuu aina edellisestä valinnasta. Piirroksesta nähdään, että esimerkiksi kirjaimen A jälkeen ei voi tulla enää kirjainta A. Prosessissa kolme tilaa. [62, s. 8]

Diskreetin informaation lähteen voidaan ajatella tuottavan muodostettavan jakson yksi symboli kerrallaan. Graafisesti esitettäessä symboli tuotetaan aina siirryttäessä tilasta toiseen. Käsillä olevasta tilanteesta riippuen symbolin valintaan vaikuttavat edelliset valinnat ja kullekin symbolille ominainen todennäköisyys. Järjestelmää, joka tuottaa jakson symboleita perustuen erilaisiin todennäköisyyksiin kutsutaan stokastiseksi prosessiksi. Edelleen voidaan osoittaa, että tietyin reunaehdoin informaation lähdettä voidaan pitää stokastisena prosessina, jossa symbo-

lin valinta riippuu ainoastaan edellisestä symbolista. Tällaista prosessia kutsutaan Markovin ketjuksi. Stokastisia prosesseja ja Markovin ketjuja on käsitelty tarkemmin luvussa 3.3.

Prosessia, joka tuottaa sellaisen symbolijonon, jonka tilastollisia ominaisuuksia kuvaa yhtä hyvin mistä tahansa jonon kohdasta irrotettu symbolijakso (pala), sanotaan ergodiseksi (tarkempi määritelmä luvussa 3.3.1). Tällöin riittävän pituinen mutta äärellinen jakso kykenee edustamaan ominaisuuksiensa puolesta mitä tahansa saman prosessin tuottamaa jaksoa. Ergodiset Markov ketjut tarjoavat hyvät edellytykset kuvata informaation lähdettä. Ergodisuus voidaan liittää prosessia kuvaaviin piirroksiin seuraavien vaatimusten kautta:

1) Kaavio ei saa sisältää toisistaan eristettyjä osioita siten, että osiosta toiseen (ja takaisin) ei kyetä siirtymään.
2) Lähdettäessä liikkeelle tilasta *i* ja seurattaessa siirtymänuolia koko ajan samaan suuntaan (esim. myötäpäivään), palataan ennen pitkään takaisin tilaan *i*. Näin muodostuneen suljetun piirin aikana tehtiin *u* kappaletta siirtymiä, eli voidaan sanoa, että piirin pituus on *u*. Toinen vaatimus ergodisuudelle on, että kaikkien kuvion suljettujen piirien suurin yhteinen jakaja saa olla yksi.

Mikäli ensimmäinen ehto täyttyy, mutta toinen ei, päädytään tilanteeseen, jossa eri jaksoilla on tilastollisesti sama rakenne huolimatta jakson alkuperästä (eli mitä symbolia pidetään jakson ensimmäisenä).

Vakaalla Markov prosessilla tarkoitetaan tilannetta, jossa prosessi on ollut toiminnassa riittävän pitkään tuottaakseen symboleita ominaisuuksiensa mukaisesti. Tällöin voidaan määrittää myös rajatodennäköisyys μ_j, millä tilasta *i* siirrytään tilaan *j*. Tämä määritellään yhtälöllä (ks. myös luku 3.3.2)

$$\mu_j = \sum_i \mu_i P_{ij} , \qquad (3.5)$$

missä μ_i = tilan *i* todennäköisyys

P_{ij} = siirtymätodennäköisyys tilasta *i* tilaan *j*.

3.2.4. Lähteen entropia

Lähteen entropialla ymmärretään lähteen kykyä tuottaa informaatiota eli mikä on entropian määrä jokaista tuotettua symbolia kohden. Lähteen entropia voidaan mieltää myös entropian tuotantonopeudeksi. Jatkossa termillä ”entropian nopeus” tarkoitetaan lähteen kykyä tuottaa

informaatiota aikayksikössä. Jos oletetaan diskreetillä informaation lähteellä olevan *i* tilaa, jotka vaikuttavat symbolin *j* valintaan, niin tällöin jokaista tilaa vastaa entropia H_i. Tällöin koko lähteen entropia määritellään yksittäisten tilojen painotettuna keskiarvona

$$H_s = \sum_i \mu_i H_i = -\sum_{i,j} \mu_i P_{ij} \log_2 P_{ij} , \qquad (3.6)$$

missä μ_i on yksittäisen tilan rajatodennäköisyys

P_{ij} on symbolin *j* ehdollinen todennäköisyys.

Mikäli lähteessä on vain yksi tila, ovat peräkkäisten symbolien valinnat riippumattomia toimenpiteitä ja tällöin lähteen entropia on yksinkertaisesti

$$H_s = -\sum_i p_i \log_2 p_i . \qquad (3.7)$$

Yhtälöt 3.6 ja 3.7 ilmoittavat lähteen entropian yksikössä bittiä/symboli. Mikäli lähde tuottaa informaatiota äärellisen ajan, voidaan entropia määrittää myös muodossa bittiä/sekunti

$$H_s^{'} = \sum_i f_i H_i , \qquad (3.8)$$

missä f_i = tilan *i* taajuus (kuinka usein keskimäärin ollaan tilassa *i*), [1/s].

Edelleen saadaan

$$H_s^{'} = \varphi_{avg} H_s , \qquad (3.9)$$

missä φ_{avg} on lähteen keskimäärin tuottamien symbolien lukumäärä sekunnissa.

3.2.5. Diskreetin kanavan kapasiteetti

Eräs tunnetuimpia informaatioteoreettisia määritelmiä on Shannonin määrittämä raja-arvo informaatiota siirtävän kanavan kapasiteetille. Edustakoon entropia $H(X)$ informaatiota (esim. symboleita), jota diskreetti informaation lähde tuottaa kanavalle ja edustakoon entropia $H(Y)$ informaatiota, joka vastaanotetaan kanavan toisella puolella. Jos oletetaan, että informaatiota siirtävään järjestelmään ei vaikuta mikään sisäinen tai ulkoinen häiriö, niin tällöin $H(X) = H(Y)$. Edelleen häiriöttömälle kanavalle pätee

$$H_s^{'} \leq C, \qquad (3.10)$$

missä C = kanavan kapasiteetti [bit/s].

Toisin sanoen diskreetin informaation lähteen entropian nopeus ei koskaan voi olla suurempi kuin on kanavan kapasiteetti.

Kuten edellä kuvattiin, voidaan informaation lähde ajatella stokastiseksi prosessiksi. Kohina (häiriöt) voidaan myös mieltää stokastiseksi prosessiksi, joka vaikuttaa informaatiota siirtävään järjestelmään. Häiriöiden vaikutus informaatioon voidaan kuvata ehdollisten entropioiden avulla. Ehdollinen entropia $H(X|Y)$ kuvaa sitä määrää alkuperäisestä informaatiosta $H(X)$, joka on jäänyt vastaanottamatta tai epävarmaksi kohinan vaikutuksesta. Ehdollinen entropia $H(Y|X)$ voidaan vastaavasti mieltää siksi osuudeksi vastaanotetusta informaatiosta $H(Y)$, joka on kohinan/häiriöiden tuottamaa. Alkuperäinen määritelmä häiriöllisen diskreetin kanavan kapasiteetille on [62, s. 22 - 23]

$$C = Max\left[H(X) - H(X \mid Y)\right], \qquad (3.11)$$

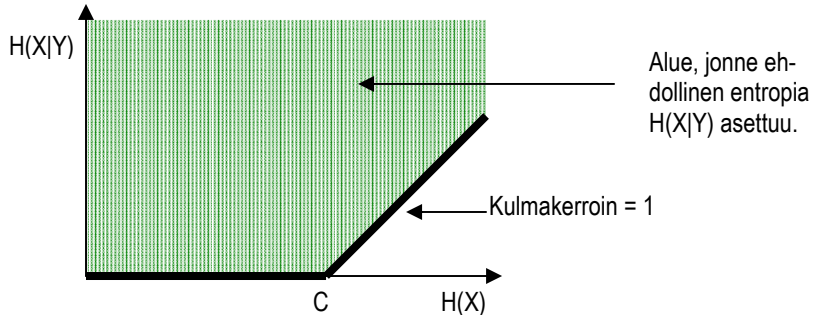
missä C = kanavan kapasiteetti [bit/s tai symbolia/s].

Lauseke $H(X) - H(X \mid Y)$ edustaa informaation lähteen todellista lähetysnopeutta R, jossa $H(X)$ edustaa informaation lähteen tuottaman informaation määrää ja $H(X|Y)$ tarkoittaa kadotetun informaation määrää. Kanavan kapasiteetin arvo määritetään suhteessa kaikkiin mahdollisiin lähteisiin, jotka tuottavat informaatiota ko. kanavalle. Jos R_n (n = 1, 2, .., k) on yksittäisen informaation lähteen todellinen lähetysnopeus, voidaan merkitä $C = Max[R_n]$.

Shannon on osoittanut, että yllä esitetty raja-arvo kapasiteetille tarkoittaa, että on muodostettavissa sellainen koodaus, jotta lähetettäessä nopeudella C, virheitä esiintyy vain haluttu määrä. Mikäli yritetään lähettää nopeudella, joka on suurempi kuin C, niin tällöin ehdollinen entropia $H(X|Y)$ on aina vähintään tuon ylityksen suuruinen. Tilanne on esitetty kuvassa 3.4. Mikäli kanava on häiriötön, on $H(X|Y) = 0$ ja päädytään yllä olevan yhtälön 3.10 tilanteeseen.

Yhtenäisinformaatio (merk. $I(X;Y)$) on esitelty luvussa 3.2.8. Tässä yhteydessä on syytä huomata, että määritelmä 3.11 voidaan lausua [16, s. 7 ja 184]

$$C = \underset{p(x)}{Max}\left[I(X;Y)\right]. \qquad (3.12)$$



Kuva 3.4: Ehdollinen entropia H(X|Y) kanavalle tuotetun entropian H(X) suhteen [62, s. 22].

3.2.6. Suhteellinen entropia

Suhteellinen entropia tarjoaa keinon vertailla kahta erilaista todennäköisyysjakaumaa. Oletetaan, että $P = (p_1,..., p_n)$ ja $Q = (q_1,..., q_n)$ ovat todennäköisyysjakaumia. Tällöin suhteellinen entropia on [36][6]

$$D_{KL}(P \parallel Q) = \sum_{i=1}^{n} p_i \log_2 \frac{p_i}{q_i}. \qquad (3.13)$$

Tyypillisesti oletetaan, että jakauma *P* on esimerkiksi tehtyihin havaintoihin perustuva ”todennettu” jakauma ja *Q* edustaa teoreettista tai muuten oletettua jakaumaa, johon ”todennettua” jakaumaa verrataan. Suhteellinen entropia on määritelty vain, jos molempien jakaumien summat ovat yksi. Lisäksi seuraavat tulkinnat ovat voimassa: $0 \log \frac{0}{0} = 0$, $0 \log \frac{0}{q} = 0$ ja $p \log \frac{p}{0} = \infty$ [16, s. 19]. Suhteelliselle entropialle käytetään yleisesti myös nimitystä Kullback – Leibler divergenssi.

Yhtälön 3.13 mukaisesti suhteellinen entropia määritellään todennäköisyysjakaumien *P* ja *Q* logaritmiseksi ja keskimääräiseksi eroksi. Keskiarvoisuus määritellään suhteessa jakaumaan *P*. Tilanteesta riippuen määritelmän 3.13 voidaan katsoa tarkoittavan mm. seuraavaa [16, s. 19], [36]:

- Kahden jakauman välinen etäisyys, jota ei kuitenkaan voida mieltää metriseksi, koska esimerkiksi symmetrisyysehto ei täyty.

[6] Alunperin yhtälö 3.13 määritteli jonkin havainnon tuottaman informaation määrän, joka puolsi hypoteesia 1 hypoteesia 2 vastaan. Informaatioon perustuva tulkinta on löydettävissä myös Rényiltä [55].

– Jakauman *P* avulla koodattuun ja kanavalle lähetettyyn sanomaan vaadittu lisäpituus (bittiä), mikäli vastaanotettaessa dekoodaukseen käytetään jakaumaa *Q*.

Suhteellisella entropialla on seuraavia ominaisuuksia [16, s. 19, 28 ja 42], [36]:

– Aina $D_{KL}(P||Q) \geq 0$.
– $D_{KL}(P||Q) = 0$ vain ja vain jos jakaumat *P* ja *Q* ovat samoja ($p_i = q_i \quad \forall i$).
– Suhteellinen entropia on sitä suurempi, mitä enemmän jakaumat poikkeavat toisistaan.
– Suhteellinen entropia ei ole symmetrinen, eli $D_{KL}(P \,||\, Q) \neq D_{KL}(Q \,||\, P)$.

3.2.7. Epätäydellisen todennäköisyysjakauman entropia

Rényi on esittänyt yleistyksen, jonka mukaisesti entropia voidaan määrittää myös epätäydellisille todennäköisyysjakaumille. Tässä luvussa on esitelty tuo yleistys [55] mukaisesti.

Olkoon $P = (p_1, p_2, ..., p_n)$ epätäydellinen todennäköisyysjakauma, jolloin pätee

$$\sum_{i=1}^{n} p_i < 1. \qquad (3.14)$$

Todennäköisyysjakauman painokerroin ilmaisee sen, kuinka epätäydellinen todennäköisyysjakauma on. Mitä lähempänä nollaa painokerroin on, sitä epätäydellisempi jakauma. Painokerroin määritetään

$$W(P) = \sum_{i=1}^{n} p_i \,, \qquad \text{jossa } 0 < W(P) \leq 1. \qquad (3.15)$$

Mikäli $W(P) = 1$, todennäköisyysjakauma *P* on täydellinen ja entropia lasketaan yhtälön 3.1 mukaisesti. Jos painokerroin on pienempi kuin yksi, on jakauma epätäydellinen, eikä yhtälön 3.1 määritelmä entropialle enää sellaisenaan kelpaa. Rényi on osoittanut, että entropia voidaan yleisesti lausua todennäköisyysjakaumalle *P*, jonka painokertoimelle pätee $0 < W(P) \leq 1$, seuraavasti

$$H_1(P) = \frac{\sum_{i=1}^{n} p_i \log_2 \frac{1}{p_i}}{\sum_{i=1}^{n} p_i}. \qquad (3.16)$$

Tämä on ns. 1-asteen entropia jakaumalle *P*. Myös useamman asteen entropioita on määritelty, mutta niitä ei tässä kohdin käsitellä.

3.2.8. Yhtenäisinformaatio (Mutual Information)

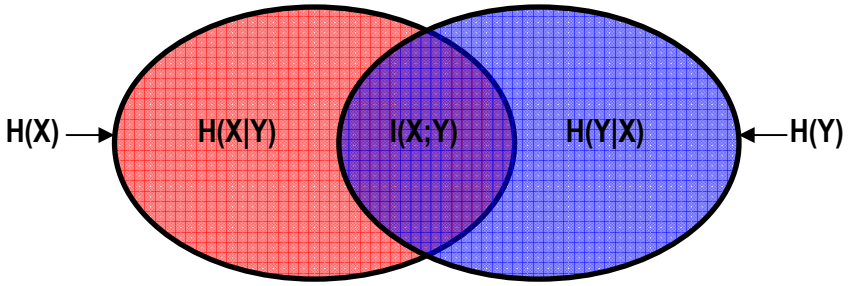
Yhtenäisinformaation perustan luo kahden satunnaismuuttujan vertailu. Jos *X* ja *Y* ovat satunnaismuuttujia, yhtenäisinformaatio *I*(*X;Y*) mittaa, kuinka paljon keskimäärin muuttujan *Y* tunteminen kertoo muuttujasta *X*, eli miten paljon satunnaismuuttujan *X* entropia (epävarmuus) vähenee, kun *Y* tunnetaan [16, s. 19 - 21]. Yhtenäisinformaatio määritellään yhtälöllä 3.17, jossa *H*(*X*) on satunnaismuuttujan *X* entropia ja *H*(*X*|*Y*) on *X*:n ehdollinen entropia, kun *Y* tunnetaan. Määritelmä on sama, kuin Shannon on teoriassaan esitellyt todelliselle lähetysnopeudelle [62, s. 21]. Kuvassa 3.5 on havainnollistettu yhtenäisinformaation suhdetta satunnaismuuttujien *X* ja *Y* entropioihin sekä ehdollisiin entropioihin.

$$I(X;Y) = H(X) - H(X \mid Y) \qquad (3.17)$$

Kuvasta 3.5 on helposti hahmotettavissa, että yhtenäisinformaatio voidaan lausua myös

$$I(X;Y) = H(X) + H(Y) - H(X,Y), \qquad (3.18)$$

missä *H(X,Y)* on *X*:n ja *Y*:n yhteisentropia.



Kuva 3.5: Yhtenäisinformaation suhde satunnaismuuttujien X ja Y entropioihin. [Co1, s. 22]

Yhtenäisinformaatiolla on useita hyödyllisiä ominaisuuksia, joita on esitelty seuraavassa. Lähteenä on käytetty [16, s. 7, 19 – 22 ja 42].

Yhtenäisinformaatiolle pätee $I(X;Y) \geq 0 \quad \forall \quad X > 0$ ja $Y > 0$. Yhtenäisinformaatio on nolla vain, jos satunnaismuuttujat *X* ja *Y* ovat riippumattomia toisistaan.

Yhtenäisinformaatio on symmetrinen, eli *X* paljastaa yhtä paljon *Y*:stä kuin *Y* paljastaa *X*:stä. Symmetrisyyden perusteella saadaan

$$I(X;Y) = H(X) - H(X \mid Y) = H(Y) - H(Y \mid X) = I(Y;X). \qquad (3.19)$$

Suhteellisella entropialla on yhtälön 3.20 mukainen yhteys yhtenäisinformaatioon.

$$I(X;Y) = D_{KL}(P(X,Y) \parallel P(X)P(Y)) \qquad (3.20)$$

Eli yhtenäisinformaatio kertoo, kuinka paljon muuttujien *X* ja *Y* yhdistetty todennäköisyysjakauma $p(x,y)$ eroaa niiden marginaalitodennäköisyysjakaumien $p(x)$ ja $p(y)$ tulosta. Yhtälö 3.20 voidaan kirjata myös muotoon

$$I(X;Y) = \sum_{x \in X} \sum_{y \in Y} p(x,y) \log \frac{p(x,y)}{p(x)\,p(y)}. \qquad (3.21)$$

3.3. Stokastiset prosessit ja Markovin ketjut

3.3.1. Markovin ketjun määritelmä ja ominaisuuksia

Tässä luvussa on esitelty matemaattiset perusteet stokastisiin prosesseihin ja erityisesti Markovin ketjuihin liittyen. Päälähteinä ovat olleet [50] ja [57]. Mahdollisesti muuhun käytettyyn kirjallisuuteen on viitattu tekstissä.

Satunnaista ilmiötä, joka kehittyy ajan kuluessa ja jota säätelevät todennäköisyyden lait, kutsutaan stokastiseksi prosessiksi. Stokastinen prosessi voidaan kuvata kokoelmaksi satunnaismuuttujia $\{X_n, n \in T\}$, missä *T* on prosessin indeksijoukko. Diskreetin stokastisen prosessin kohdalla indeksijoukko *T* muodostuu tyypillisesti kokonaisluvuista $T = \{0, \pm 1, \pm 2, ...\}$ tai luonnollisista luvuista $T = \{0,1,2,...\}$. Hyvin usein indeksijoukko kuvaa ajanhetkiä, joita kutakin vastaa jokin satunnaismuuttujan X_n arvo; esimerkiksi ajanhetkellä t_n (missä $n = 0$) satunnaismuuttujan arvo on $X_0 = i_0$. Tällöin rinnastetaan, että prosessi on *tilassa* i_0 ajanhetkellä t_0. Sto-

kastisen prosessin *tila-avaruus* määritellään joukoksi, joka sisältää kaikki mahdolliset satunnaismuuttujan X_n arvot. Jatkuvan stokastisen prosessin indeksijoukko on tyypillisesti määritelty kattamaan reaaliluvut $T = \{-\infty < n < \infty\}$ tai positiiviset reaaliluvut $T = \{n \geq 0\}$. Indeksijoukko voi olla myös jokin väli $T = \{a < n < b\}$.

Järjestelmä, joka on todettu stokastiseksi prosessiksi, voidaan nimetä Markov prosessiksi, mikäli se noudattaa seuraavia ehtoja: todennäköisyys sille, että järjestelmä tulee olemaan tietyssä *tilassa* ajanhetkellä t_2, voidaan johtaa tietämällä järjestelmän *tila* hetkellä t_1, eikä järjestelmän tilalla ennen hetkeä t_1 ole merkitystä. Mikäli Markov prosessin tila-avaruus on äärellinen tai numeroituvasti ääretön, voidaan prosessista käyttää nimitystä Markovin ketju.

Jos oletetaan että stokastinen prosessi $\{X_n, n = 0,1,2,...\}$ on Markovin ketju, niin tällöin pätee

$$P[X_{n+1} = j \mid X_n = i, X_{n-1} = i_{n-1}, ..., X_1 = i_1, X_0 = i_0] = P_{ij} \qquad (3.22)$$

kaikille tiloille $i_0, i_1, \ldots, i_{n-1}, i, j$ ja kaikille $n \geq 0$. Todennäköisyys P_{ij} edustaa siirtymätodennäköisyyttää sille, että ollessaan hetkellä n tilassa i, järjestelmä siirtyy seuraavaksi tilaan j. Toisin sanoen, Markovin ketjun ehdollinen todennäköisyysjakauma mille tahansa tulevalla tilalle X_{n+1} riippuu ainoastaan nykyisyyden tilasta X_n, eikä menneisyyden tiloista $X_0, X_1, \ldots, X_{n-1}$. Yllä oleva määritelmä 3.22 voidaan näin ollen kirjata muotoon:

$$P_{ij} = P[X_{n+1} = j \mid X_n = i]. \qquad (3.23)$$

Koska todennäköisyydet ovat aina positiivisia ja koska prosessin täytyy aina jatkaa siirtymistä johonkin tilaan, pätevät seuraavat toteamat:

$$P_{ij} \geq 0, \qquad (3.24a) \qquad \sum_{j=0}^{\infty} P_{ij} = 1. \qquad (3.24b)$$

Tilojen[7] i ja j väliset siirtymätodennäköisyydet P_{ij} esitetään yleensä todennäköisyysmatriiseina alla esitetyn mukaisesti

[7] Tilatunnukset *i* ja *j* esitetään monesti lukuina, vaikka ne voivat periaatteessa olla mitä tahansa symboleita (ks. esim. alla).

$$\mathrm{P} = \begin{pmatrix} P_{00} & P_{01} & \cdots & P_{0j} \\ P_{10} & P_{11} & \cdots & P_{1j} \\ \vdots & \vdots & \ddots & \vdots \\ P_{i0} & P_{i1} & \cdots & P_{ij} \end{pmatrix}. \tag{3.25}$$

Esimerkkinä Markovin ketjusta mainittakoon kirjainjonon muodostaminen, jossa ensimmäinen kirjain valitaan satunnaisesti kirjan ensimmäiseltä sivulta ja tätä seuraava kirjain valitaan seuraavalta sivulta lukemalla niin pitkään, että edellinen kirjain löydetään ja valitsemalla sitten viereinen (oikealla puolella oleva) kirjain[8]. Prosessi toistetaan seuraavalle kirjaimelle. Tällöin seuraavan kirjaimen valinta riippuu ainoastaan sitä edellisestä kirjaimesta, eikä aikaisemmilla valinnoilla ole merkitystä. Jos oletetaan, että kirja on ymmärrettävää suomen kieltä, ja halutaan muodostaa siirtymätodennäköisyysmatriisi, tulee olla käytössä tilastot, jotka ilmaisevat erilaisten kirjainyhdistelmien taajuudet suomen kielessä. Esimerkiksi kirjainyhdistelmä JA on varmasti paljon yleisempi kuin yhdistelmä VV[9]. Tällaisesta prosessista saadaan rakennettua siirtymätodennäköisyysmatriisi $\mathbf{P}_\mathrm{K}$ seuraavasti:

$$\mathrm{P}_K = \begin{pmatrix} P_{AA} & P_{AB} & P_{AC} & \cdots & P_{A\ddot{O}} \\ P_{BA} & P_{BB} & P_{BC} & \cdots & P_{B\ddot{O}} \\ P_{CA} & P_{CB} & P_{CC} & \cdots & P_{C\ddot{O}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ P_{\ddot{O}A} & P_{\ddot{O}B} & P_{\ddot{O}C} & \cdots & P_{\ddot{O}\ddot{O}} \end{pmatrix}. \tag{3.26}$$

Matriisin 3.26 ensimmäinen rivi vastaa tilannetta, jossa ollaan tilassa A (sivulla, jossa on valittu A kirjain). Esimerkiksi siirtymätodennäköisyys P_{AA} kertoo, millä todennäköisyydellä seuraavalta sivulta valittava kirjain on myös A. Matriisissa esitetyt todennäköisyydet ovat ehdollisia, koska nimenomaisesti painotetaan erilaisten kirjainyhdistelmien *ij* esiintymistiheyttä suomenkielisessä tekstissä.

Tilanne on oleellisesti erilainen, mikäli tekstin ymmärrettävyys ei ole vaatimuksena, vaan kirjaimet ovat satunnaisessa järjestyksessä noudatellen kuitenkin tyypillisiä esiintymistiheyksiä suomenkieliselle tekstille. Käytännössä eri sivuilta valituksi tulevat kirjaimet ovat tällöin toisistaan riippumattomia ja kunkin kirjaimen yleisyyttä kuvaavat tilastolliset todennäköisyydet voidaan esittää vektorina. Alla esitettyyn rivivektoriin 3.27 on esimerkkinä kirjattu muutamien

[8] Esimerkki on sovellus teoksessa [62] esitetystä.
[9] Väite ei perustu tutkittuun tietoon, vaan vahvaan mielikuvaan. Huomattakoon, että sana JA on suomen kielen toiseksi yleisin sana [60], kun taas sanoja joissa esiintyy yhdistelmä VV tai edes sanoja, jotka päättyvät kirjaimeen V on varsin vaikea löytää.

suomen kielessä esiintyvien kirjaimien tilastollisia todennäköisyyksiä. Kirjainten esiintymistiheydet ovat lähteen [54] mukaiset.

$$\mathrm{P} = \begin{pmatrix} P_A & P_B & \cdots & P_{Ö} \end{pmatrix} = \begin{pmatrix} 0.1190 & 0.0006 & \cdots & 0.0049 \end{pmatrix} \qquad (3.27)$$

Edellä on määritetty siirtymätodennäköisyyksiä tilanteissa, joissa tilan *j* oletetaan olevan heti seuraava tila, johon nykyisestä tilasta *i* siirrytään. Chapman-Kolomogorov yhtälöllä (3.28) voidaan laskea todennäköisyys, että oltaessa tilassa *i* saavutetaan tila *j* *n*-askeleen jälkeen, eli tilojen *i* ja *j* välillä on *n* siirtymää.

$$P_{ij}^{n+m} = \sum_{k=0}^{\infty} P_{ik}^{n} P_{kj}^{m} \qquad \forall n, m \geq 0, \quad \forall i, j \qquad (3.28)$$

Yllä oleva voidaan mieltää siten, että $P_{ik}^{n} P_{kj}^{m}$ kuvaa todennäköisyyttä, jossa prosessi lähtee liikkeelle tilasta *i* ja siirtyy *n*+*m* siirtymällä tilaan *j*. Reitti kulkee tilan *k* kautta, jonka etäisyys tilasta *i* on *n* siirtymää. Voidaan osoittaa, että *n*-askeleen siirtymätodennäköisyysmatriisi $\mathbf{P}^{(n)}$ saadaan kertomalla matriisi **P** itsellään *n* kertaa, eli

$$\mathrm{P}^{(n)} = \mathrm{P}^{n}. \qquad (3.29)$$

Matriisien laskentasääntöjä ei tässä yhteydessä käsitellä, vaikka niitä luvussa 4 tullaan käyttämään. Lisätietoja löytyy mm. [2], [47] ja [57].

Markov ketjun sanotaan olevan redusoitumaton (irreducible), mikäli kaikki sen tilat kommunikoivat keskenään. Toisin sanoen tilasta *i* on päästävä siirtymään suoraan tai välillisesti jonkin muun/muiden tilojen kautta kaikkiin muihin prosessin tiloihin. Ergodisella prosessilla määritellään olevan seuraavat ominaisuudet:

- positiivisesti toistuva (positive recurrent), eli lähdettäessä liikkeelle tilasta *i*, voidaan odottaa paluuta takaisin ko. tilaan äärellisen ajan kuluessa
- jaksoton (aperiodic), eli kaikkien prosessin suljettujen piirien suurin yhteinen jakaja on 1 (vrt. luku 3.2.3).

Voidaan osoittaa, että redusoitumattomalle ja ergodiselle äärellisen määrän tiloja omaavalle Markovin ketjulle on olemassa raja-arvo $\lim_{n\to\infty} P_{ij}^{n}$ ja se on riippumaton lähtötilasta *i*. Toisin

sanoen, on löydettävissä rajatodennäköisyydet μ_j, joita siirtymätodennäköisyydet lähestyvät, kun askelten määrä $n \to \infty$. Rajatodennäköisyys määritellään siis

$$\mu_j = \lim_{n\to\infty} P_{ij}^n . \qquad (3.30)$$

Edelleen pätee (vrt. luku 3.2.3)

$$\mu_j = \sum_i \mu_i P_{ij} \qquad \text{ja} \qquad (3.31)$$

$$\sum_j \mu_j = 1 . \qquad (3.32)$$

Rajatodennäköisyyksien avulla voidaan Markov ketjulle määrittää ns. vakaa todennäköisyysjakauma (μ), joka kertoo millä todennäköisyydellä vakaa prosessi on tilassa *j* *n*-askeleen jälkeen. Vakaa todennäköisyysjakauma voidaan tulkita myös pitkällä aikavälillä suhteelliseksi ajaksi, jonka prosessi kussakin tilassa viettää.

3.3.2. Eräitä informaatioteoreettisia ominaisuuksia Markov ketjuille

Luvussa 3.2.3 on käsitelty Markovin ketjuja diskreetin informaation lähteen näkökulmasta ja tässä yhteydessä on esitetty joitakin Markov ketjujen ominaisuuksia. Tässä luvussa esitellään muutamia muita mielenkiintoisia ja hyödyllisiä ominaisuuksia, jotka pätevät suljetulle järjestelmälle, jonka tilat ovat tulosta Markov ketjusta. Ominaisuuksien tarkempia perusteluita ei ole esitetty. Perustelut ovat löydettävissä esimerkiksi tämän luvun perusteena käytetystä teoksesta [16, s. 71 - 88].

Suhteellinen entropia $D_{KL}(\rho_n \parallel \rho_n^{'})$ kahden samalla hetkellä *n* muodostetun todennäköisyysjakauman välillä vähenee, kun *n* kasvaa.

Suhteellinen entropia $D_{KL}(\rho_n \parallel \mu)$ vähenee, kun aika *n* kasvaa. Tässä ρ_n on Markov ketjun tuottama todennäköisyysjakauma eri tiloille hetkellä *n* ja μ on prosessin vakaa todennäköisyysjakauma. Eli ajan kuluessa Markov ketjun tuottama todennäköisyysjakauma lähestyy vakaata todennäköisyysjakaumaa. Mikäli vakaa todennäköisyysjakauma on täydellinen, niin $D_{KL}(\rho_n \parallel \mu) \to 0$ kun $n \to \infty$.

Järjestelmän entropia kasvaa, jos vakaa todennäköisyysjakauma μ on tasajakauma. Suhteellisen entropian väheneminen ei näin ollen välttämättä tarkoita entropian vähentymistä. Järjestelmän entropia voi myös vähentyä, jos vakaa todennäköisyysjakauma ei ole tasajakauma.

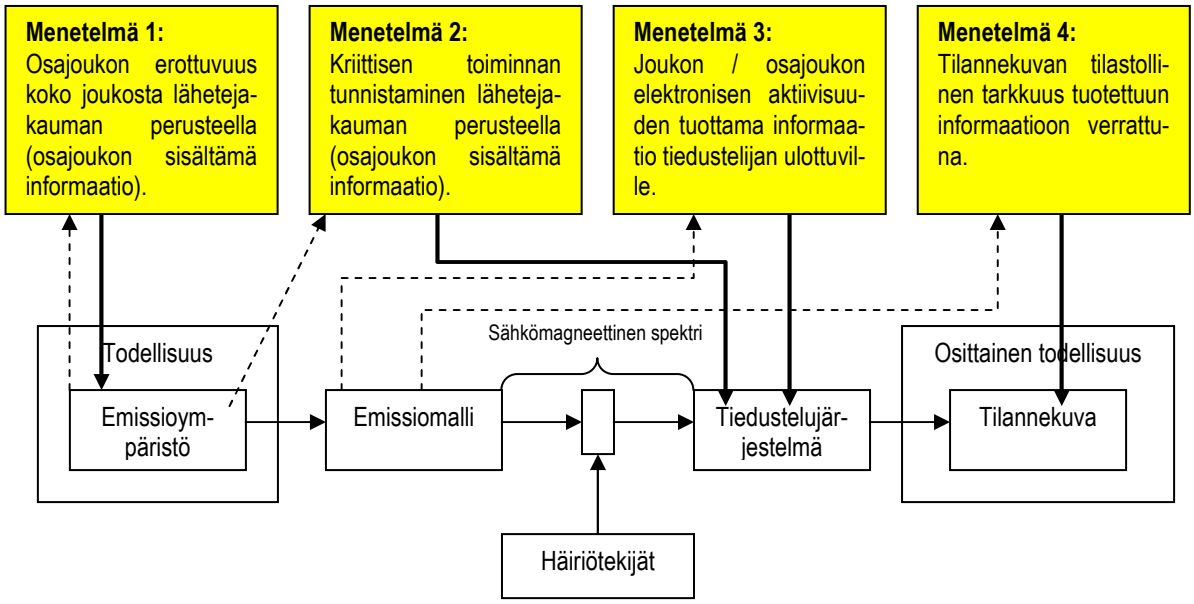
Vakaalla Markov prosessilla ehdollinen entropia $H(X_n|X_1)$ kasvaa, kun n kasvaa. Näin on, vaikka vakaalla Markov prosessilla entropia $H(X_n)$ on vakio. Toisin sanoen, ehdollinen epävarmuus tulevasta kasvaa, kun aika kuluu.

4. MENETELMIÄ OSAJOUKON ELEKTRONISEN AKTIIVISUUDEN ARVIOIMISEKSI

4.1. Käsittelyn kokonaisuus ja käsitteet

4.1.1. Menetelmien näkökulmat ja sijoittuminen kokonaisuuteen

Tässä työssä tullaan esittelemään neljä erilaista informaatioteorian määritelmiin pohjautuvaa menetelmää, joita voidaan hyödyntää arvioitaessa joukon ja osajoukon elektronista aktiivisuutta sekä elektronisen suojautumisen tasoa. Kaikki neljä menetelmää ovat itsenäisiä tarkastelleen elektronista aktiivisuutta hieman eri näkökulmista. Informaatioteoreettisen näkökulman kokonaisuutta hahmoteltiin jo luvussa 1.2. Kokonaiskuvaa voidaan tarkentaa sijoittamalla esiteltävät menetelmät kuvassa 4.1 havainnollistetulla tavalla tilannekuvan muodostumista kuvaavaan malliin. Alla on lyhyesti kuvattu kunkin menetelmän tarkoitusta ja näkökulmaa.



Kuva 4.1: Elektronisen aktiivisuuden arviointiin tarkoitettujen menetelmien sijoittuminen informaation kuvautumista mallintavan järjestelmän eri vaiheisiin. Katkoviivalla on kuvattu syöte vaiheesta, jonka perusteella menetelmälle määritellään informaation alkuperäinen määrä (vallitsevassa todellisuudessa olevan tai tuotetun informaation määrä).

Luvussa 4.2 tullaan esittelemään kaksi menetelmää, joiden avulla voidaan arvioida osajoukkojen (ja joukon) sisältämän informaation määrää ja sen vaikutuksia osajoukon tunnistettavuuteen. Menetelmä 1 käsittelee joukon organisaatiorakenteen ja siihen sidoksissa olevan kalustollisen jakauman analysointia. Tässä käsittelyssä kalustolla ymmärretään kaikkia sähkömag-

neettista säteilyä lähettäviä laitteita, jotka kuuluvat organisaation tiedonsiirto- ja sensorijärjestelmiin. Tullaan osoittamaan, että analysoimalla eri osajoukkojen sisältämän entropian määrä, kyetään löytämään eniten sormenjälkiä spektriin jättävät osajoukot. Menetelmä 2 keskittyy analysoimaan, miten hyvin jokin osajoukon maantieteellisesti rajatulla alueella toteuttama toiminta erottuu ympäristöstään kalustollisen jakauman näkökulmasta. Tullaan osoittamaan, että yhtenäisinformaatiota hyödyntämällä voidaan tällainen mitallinen arvio tuottaa.

Kolmas osakokonaisuus (luku 4.3) esittelee emissiomallin, jonka avulla kuvataan osajoukon sähkömagneettiseen spektriin tuottamaa informaation määrää. Yhtenäisinformaatiota soveltamalla arvioidaan, kuinka paljon tuosta tuotetusta informaatiosta on tiedustelijan käytettävissä. Ehdollisen entropian avulla täydennetään yhtenäisinformaatiota soveltamalla saatuja tuloksia. Käsittelyyn liittyvät olennaisesti signaalin havaitsemiseen ja hyödyntämiseen liittyvät tekijät. Hyödyntäminen on tässä käsittelyssä rajattu koskemaan vain paikannustarkkuutta. Emissiomallit rakennetaan vain tiedonsiirtojärjestelmiä varten. Sensorijärjestelmien (tutkat) kuvaaminen tässä työssä esiteltävillä emissiomalleilla ei ole hyödyllistä.

Neljännen menetelmän (luku 4.4) perustan luo oletus, jonka mukaan tiedustelijan luoman tilannekuvan tarkkuutta voidaan arvioida tilastollisia todennäköisyysjakaumia vertailemalla. Tämän oletuksen varassa on esitelty suhteellista entropiaa hyödyntävä menetelmä, jota voidaan käyttää elektronisen aktiivisuuden ja elektronisen suojautumisen arvioinneissa.

Luvussa 5 esitetyt menetelmät laajennetaan käsittelemään soveltuvilta osin koko joukkoa.

4.1.2. Käsitteitä

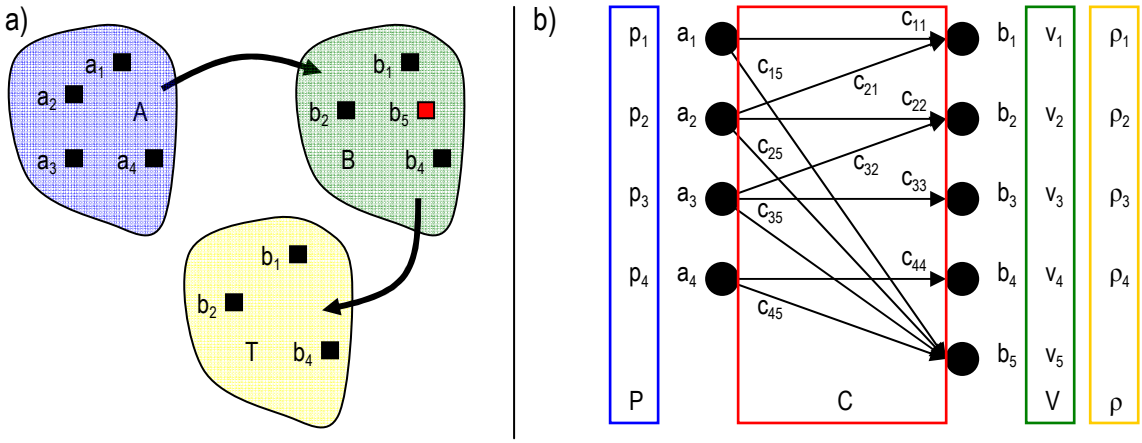
Informaatioteoreettinen käsittely perustuu mitä suurimmassa määrin eri tavoin määritellyille todennäköisyysjakaumille. Erilaisia todennäköisyyskäsitteitä esiintyykin tulevissa luvuissa runsaasti. Tässä luvussa on esitelty tärkeimmät käsitteet.

Lähetetodennäköisyys kuvaa yksittäisen lähettimen yleisyyttä tarkastelun kohteena olevassa joukossa. Jos samantyyppisiä lähettimiä on runsaasti ko. joukossa, on lähetetodennäköisyys pieni. Lähetetodennäköisyys on suhteessa suurempi lähettimillä, joita on vain muutamia tarkasteltavassa joukossa tai jos lähetteessä on jokin anomalia, joka erottaa sen muista samantyyppisistä lähettimistä. Lähetetodennäköisyyttä hyödynnetään arvioitaessa osajoukon tai jon-

kin toiminnan erottumista emissioympäristöstä. Yksityiskohtaisempi määrittely on esitelty luvussa 4.2.2.

Lähetetodennäköisyysjakauma on diskreetti todennäköisyysmassafunktio, joka muodostetaan osajoukkoon tai tiettyyn toimintaan sisältyvien lähettimien lähetetodennäköisyyksien pohjalta. Jakaumaa käytetään ko. osajoukon tai toiminnan sisältämän informaation (entropian) määrän selvittämiseen.

Seuraavaksi esiteltävien käsitteiden hahmottamista selventävät kuvat 4.2 a ja b.



Kuva 4.2: a) Lähtöjoukko A sisältää symbolit (lähettimet/lähetteet) a_1 – a_4. Tulojoukko B on kanavan yli kuvautuneiden symbolien joukko. Tilannekuvajoukko T on tiedustelujärjestelmän muodostama tilannekuva lähtöjoukosta A. b) Lähtöjoukon symbolien (a_1 – a_4) kuvautuminen tulojoukon symboleiksi (b_1 – b_5). Kuvautuminen tapahtuu oikein todennäköisyydellä c_{ij}, missä i = j (esim. c_{11}). Tulojoukon symboli b_5 on tyhjä symboli (välilyönti), joka kuvaa häiriöiden vaikutuksesta hävinneitä symboleita. Tietyissä olosuhteissa lähtöjoukon symbolit voivat kuvautua myös vääriksi tulojoukon symboleiksi ($i \neq j$). **Selitteet: P = esiintymistodennäköisyydet, C = kuvautumistodennäköisyydet, V = vastaanottotodennäköisyydet ja ρ = tiedustelutodennäköisyydet.**

Lähtöjoukko (ks. kuva 4.2 a)) on todellinen emissioympäristö, joka voi sisältää erinäisen määrän erityyppisiä lähettimiä (symboleja). Lähtöjoukko on monesti rajattu sisältämään tarkastelun kohteena olevan osajoukon tai toiminnan lähettimet. Lähtöjoukon lähettimien aktiivisuutta sähkömagneettisen spektrin suhteen kuvataan emissiomallilla.

Tulojoukko (ks. kuva 4.2 a)) muodostuu lähtöjoukon symbolien kuvautuessa mahdollisesti häiriöllisen kanavan yli. Tiedustelujärjestelmä pyrkii keräämään informaatiota sähkömagneettisesta spektristä juuri sellaisen määrän, kuin lähtöjoukko on sinne tuottanut. Erilaiset fysikaaliset, tekniset ja toiminnalliset ilmiöt kuitenkin vaikeuttavat informaation keräämistä eikä tiedustelujärjestelmän ulottuvilla oleva informaatio ole enää sama verrattuna lähtöjoukon tuot-

tamaan. Lähtöjoukon tuottaessa symboleita (lähetteitä) jonkin äärellisen ajan, tulee juuri sama määrä symboleita kuvautua myös tulojoukkoon. Kuvautumistodennäköisyyksien vaikutuksesta kuvautuneiden symboleiden järjestys ei välttämättä enää ole sama kuin lähetettäessä tai osa lähetetyistä symboleista on voinut häiriöiden takia hävitä ja näin ollen ne on korvattu hävinneitä symboleita kuvaavalla symbolilla ”välilyönti”.

Tilannekuvajoukko (ks. kuva 4.2 a)) on tiedustelujärjestelmän muodostama tilannekuva lähtöjoukosta. Tilannekuvajoukko muodostetaan tulojoukon sisältämän informaation pohjalta kuitenkin siten, että häiriöiden johdosta hävinneitä symboleita ei enää huomioida. Toisin sanoen, se mitä tiedustelujärjestelmä ei ole kyennyt vastaanottamaan ei myöskään käytetä tilannekuvan muodostamiseen.

Esiintymistodennäköisyys (ks. kuva 4.2 b)) ilmaisee lähtöjoukon symbolin (lähettimen) suhteellista aktiivisuutta verrattuna muihin lähtöjoukon symboleihin. Toisin sanoen esiintymistodennäköisyys kuvaa symbolin tilastollista osuutta emissiomallin tuottamassa symbolijonossa. Esiintymistodennäköisyysjakauma on diskreetti todennäköisyysmassafunktio, joka muodostetaan lähtöjoukon symboleiden esiintymistodennäköisyyksistä. Emissiomalli voidaan muodostaa tähän jakaumaan perustuen etenkin, jos peräkkäisten symbolien järjestystä ei ole mitenkään rajoitettu. Malleissa, joissa symboleiden esiintymistä on rajoitettu, rajatodennäköisyydet (ks. luku 3.3.1) vastaavat esiintymistodennäköisyyksiä. Esiintymistodennäköisyysjakauman avulla voidaan määrittää lähtöjoukon informaation (entropian) määrä.

Kuvautumistodennäköisyys (ks. kuva 4.2 b)) kertoo, millä todennäköisyydellä lähtöjoukon symboli kuvautuu kanavan yli tietyiksi tulojoukon symboleiksi. Symbolin kuvautuminen on yksikäsitteinen (kuvautumistodennäköisyys c_{ij} (missä $i = j$) on 1), mikäli mikään fysikaalinen, tekninen tai toiminnallinen häiriötekijä ei vaikuta kuvautumiseen. Häiriötekijät voivat aiheuttaa symboleiden häviämisiä tai niiden kuvautumista vääriksi tulojoukon symboleiksi. Kuvautumistodennäköisyyksien muodostumista on käsitelty erikseen luvussa 4.3.3.

Vastaanottotodennäköisyys (ks. kuva 4.2 b)) ilmaisee kanavan yli kuvautuneen symbolin suhteellisen osuuden verrattuna muihin tulojoukon symboleihin. Toisin sanoen vastaanottotodennäköisyys kuvaa symbolin tilastollista osuutta kanavan yli kuvautuneessa symbolijonossa. Vastaanottotodennäköisyysjakauma on diskreetti todennäköisyysmassafunktio, joka muodostetaan vastaanottotodennäköisyyksien mukaisesti. Jakaumassa huomioidaan myös hävinneiden

(”välilyönti”) symboleiden osuus. Vastaanottotodennäköisyysjakauman avulla voidaan määrittää tiedustelujärjestelmän ulottuvilla olevan informaation (entropian) määrä.

Tiedustelutodennäköisyys (ks. kuva 4.2 b)) kertoo tilannekuvajoukon symbolin suhteellisen osuuden verrattuna muihin tilannekuvajoukon symboleihin. Tiedustelutodennäköisyysjakauma on diskreetti todennäköisyysmassafunktio, joka kuvaa vastaanotettujen symbolien suhteellista keskinäistä jakaumaa, kun ei enää huomioida menetettyjä symboleita (”välilyöntejä”). Jakauman avulla voidaan arvioida tuotetun tilannekuvan tarkkuutta.

Käytettävyystodennäköisyys kuvaa millä todennäköisyydellä yksittäinen emissiomallin tuottama symboli (lähete) saadaan tiedustelujärjestelmän käyttöön. Käytettävyystodennäköisyydessä yhdistyvät näin ollen kaikkien häiriötekijöiden vaikutus. Häiriötekijät voidaan määrittää sieppaus-, ilmaisu- ja hyödyntämistodennäköisyyksien avulla. Käytettävyystodennäköisyyksien avulla määritetään kuvautumistodennäköisyydet. Tätä problematiikka on tarkemmin käsitelty luvussa 4.3.3.

4.2. Tunnistaminen

4.2.1. Tunnistamisen lähtökohdat

Kuten luvussa 2.2.2 on kerrottu, erilaisten signaalien tunnistaminen perustuu varsin usein sen teknisiin parametreihin. Tunnistaminen voi toki perustua myös inhimillisiin parametreihin, kuten viestittäjän äänen tai sähkötystyylin tunnistamiseen. Selväkielinen tai heikosti salattu (realistisessa ajassa avattavissa oleva) viestiliikenne saattaa myös paljastaa esimerkiksi joukon, jolle laite kuuluu tai muita joukon toiminnan ja suunnitelmien kannalta kriittistä tietoa. Erilaiset anomaliat lähetteissä saattava helposti jopa identifioida yksittäisen laitteen kuuluvaksi johonkin tiettyyn lavettiin tai tietylle joukolle. Anomalioita saattavat aiheuttaa esimerkiksi erot laitteiden komponenteissa tai laiteviat.

Lähtökohta esitetylle käsittelylle on, että erilaiset lähetteet kyetään luokittelemaan kuuluvaksi tiettyihin lähetekategorioihin teknisten parametriensa mukaisesti. Varsinaista tunnistamista käsitellään osajoukkoon liittyvänä ilmiönä, jossa erilaisten laitteiden/lähetteiden jakauma osajoukossa määrittää osajoukon sisältämän informaation määrän. Informaation määrään sitoen voidaan arvioida erilaisten osajoukkojen erottuvuutta suhteessa muihin osajoukkoihin ja toimintoihin.

4.2.2. Osajoukkojen vertailu painokertoimien ja entropioiden avulla

Tarkasteltavan joukon eri tasoille asettuvia osajoukkoja voidaan vertailla perustuen kullekin osajoukolle kuuluvaan kalustoon. Tavoitteena on saada kokonaiskäsitys siitä, miten hyvin erilaiset osajoukot erottuvat toisistaan ja millainen on eritasoisten osajoukkojen vaikutus koko joukon tunnistettavuuden kannalta. Vertailua varten muodostetaan taulukko (joukko-lähete –taulukko), jossa käsiteltävä joukko esitetään niin pieniksi osajoukoiksi jaettuna, kuin halutaan tarkastelun ulottuvan. Taulukon avulla linkitetään erilaiset laitteet ja lähetintyypit (lähetekategoriat) kuulumaan oikealle osajoukolle. Joukko-lähete –taulukon periaate on esitetty taulukossa 4.1. Mitä yksityiskohtaisemmin kalustot ja erityyppiset lähetteet kyetään erottelemaan, sitä tarkempi tarkastelu saadaan laadittua. Näin ollen kaikki tiedossa olevat ”erikoisuudet” lähetteissä on eroteltava omaksi lähetekategoriakseen. Lähetekategoria on oleellinen käsite esiteltävien tarkasteluiden kannalta. Lähetekategorian muodollinen määritelmä on esitetty alla.

	L1	L2	L3	…	Lk	∑
Joukko (JO0)	S_0^{L1}	S_0^{L2}	S_0^{L3}	…	S_0^{Lk}	S_0
Osajoukko (OJ1.0)	$S_{1.0}^{L1}$	$S_{1.0}^{L2}$	$S_{1.0}^{L3}$	…	$S_{1.0}^{Lk}$	$S_{1.0}$
- Osajoukko (OJ1.1)	$S_{1.1}^{L1}$	$S_{1.1}^{L2}$	…	…	$S_{1.1}^{Lk}$	$S_{1.1}$
- Osajoukko (OJ1.2)	$S_{1.2}^{L1}$	…	…	…	$S_{1.2}^{Lk}$	$S_{1.2}$
Osajoukko (OJ2.0)	$S_{2.0}^{L1}$	…	…	…	$S_{2.0}^{Lk}$	$S_{2.0}$
- Osajoukko (OJ2.1)	$S_{2.1}^{L1}$	…	…	…	$S_{2.1}^{Lk}$	$S_{2.1}$
- Osajoukko (OJ2.1.1)	$S_{2.1.1}^{L1}$	…	…	…	$S_{2.1.1}^{Lk}$	$S_{2.1.1}$
- Osajoukko (OJ2.1.2)	$S_{2.1.2}^{L1}$	…	…	…	$S_{2.1.2}^{Lk}$	$S_{2.1.2}$
Jne…	…	…	…	…	…	

Selitteet:
L1 – Lk = lähetekategoriat
k = kategorioiden lukumäärä
S_r^{Ln} = lähettimien määrä ko. kategoriassa ja osajoukossa/joukossa
Ln = lähetekategorian tunnus
S_r = lähettimien määrä yhteensä joukossa / osajoukossa
r = joukon / osajoukon tunnus

Taulukko 4.1: Lähettimien määrä lähetekategorioittain eri osajoukoille. Ylemmän osajoukon/joukon lähettimien määrä on sen alijoukkojen lähettimien summa: esim. $S^{L1}_{1.0}=S^{L1}_{1.1}+S^{L1}_{1.2}$ ja $S^{L1}_{2.1} = S^{L1}_{2.1.1} + S^{L1}_{2.1.2}$.

Määritelmä - Lähetekategoria

Olkoon $X = \{x_1, x_2, ..., x_m\}$ joukko emissioympäristön lähettimiä, jotka on jaoteltu siten, että samantyyppiset lähettimet ovat peräkkäin. Erotetaan peräkkäin järjestetyt lähettimet osajoukoiksi $X_{L1}, X_{L2}, ..., X_{Lk} \subset X$ siten, että kuhunkin osajoukkoon sisältyy vain yhden tyyppisiä lähettimiä. Lisäksi vaaditaan, että kaikki samantyyppiset lähettimet kuuluvat samaan osajoukkoon. Nyt pätee

$$\bigcap_{n=1}^{k} X_{Ln} = \varnothing \text{ ja } \bigcup_{n=1}^{k} X_{Ln} = X .$$

Näin muodostettuja yksittäisiä osajoukkoja X_{Ln} kutsutaan lähetekategorioiksi. *Ln* on kategorian tunnus. ◇

Lähetekategorioihin pohjautuen voidaan määritellä lähetetodennäköisyys, jolla kuvataan yksittäisen lähettimen yleisyyttä osana koko joukkoa. Lähetetodennäköisyyden muodollinen määritelmä on esitetty seuraavassa.

Määritelmä – Lähetetodennäköisyys

Olkoon $X = \{x_1, x_2, ..., x_m\}$ joukko emissioympäristön lähettimiä, jotka voidaan jakaa *k* kappaleeseen lähetekategorioita. Merkitään kuhunkin lähetekategoriaan X_{Ln} sisältyvien lähettimien kokonaislukumäärää S_0^{Ln}, missä *n* = 1, …, *k*. Yksittäisen kategoriaan *Ln* kuuluvan lähettimen todennäköisyys tulla valituksi kaikkien ko. kategoriaan kuuluvien lähettimien joukosta on $1/S_0^{Ln}$. Saatu suhde normalisoidaan koko joukon suhteen jakamalla kategorioiden lukumäärällä *k*. Nyt saadaan

$$P_{Ln} = \frac{1}{kS_0^{Ln}}, \qquad (4.1)$$

missä $S_0^{Ln} \neq 0$ ja $k \neq 0$.

Suhdetta P_{Ln} nimitetään lähetetodennäköisyydeksi ja se kuvaa yksittäisen lähettimen yleisyyttä koko joukossa *X*. ◇

Osajoukkojen lähetejakauman kokonaisuutta voidaan arvioida jakauman painokertoimien ja entropioiden avulla. Edellä määritellyt lähetetodennäköisyydet muodostavat kullekin osajoukolle tyypillisen diskreetin lähetetodennäköisyysjakauman $P_r = (p_1, p_2, ..., p_{S_r})$, jossa siis todennäköisyydet $p_1 ... p_{S_r}$ ovat suoraan kullekin lähetinyksilölle määritetty lähetetodennäköisyys P_{Ln}. Alaindeksillä *r* kuvataan osajoukon tunnusta, esim. $P_{1.0}$. Tarkasteltaessa näin muodostettuja lähetetodennäköisyysjakaumia havaitaan, että ne ovat osajoukkojen kyseessä ollessa aina epätäydellisiä eli $\sum_{i=1}^{S_r} p_i < 1$, kun $r \neq 0$. Koko joukosta ($r = 0$) muodostettu lähetetodennäköisyysjakauma on täydellinen eli erillisten todennäköisyysarvojen summa on yksi. Edellä luvussa 3.2.7 esiteltiin määritelmä (yhtälö 3.15) todennäköisyysjakauman painokertoimelle. Painokerroin voidaan vastaavasti määritellä lähetetodennäköisyysjakaumille seuraavasti:

$$W(P_r) = \sum_{i=1}^{S_r} p_i \ . \qquad (4.2)$$

Yllä esitetyn perusteella koko joukon painokerroin on $W(P_0) = 1$ ja jokaiselle osajoukolle pätee $0 < W(P_r) < 1$[10]. Osajoukon painokerroin on aina alijoukkojensa summa, joten myös koko joukon painokerroin on suoranaisten osajoukkojen summa. Osajoukon painokerroin kertoo, kuinka paljon koko joukon todennäköisyysmassasta on absoluuttisesti sitoutunut kuhunkin osajoukkoon. Osajoukon suuri painokerroin voi olla merkki kahdesta ominaisuudesta: 1) osajoukolla on runsaasti lähettimiä verrattuna muihin osajoukkoihin tai 2) osajoukolla on lähettimiä, joiden lähetetodennäköisyydet ovat suuria. Tunnistamisen kannalta erityisesti jälkimmäinen tilanne on mielenkiintoinen, koska tällöin osajoukon ja mahdollisesti jopa koko joukon tunnistaminen saattaa olla helppoa muutamiin selkeästi organisaatiosta erottuviin lähetteisiin perustuen.

Edellä todettiin, että osajoukkojen lähetetodennäköisyysjakaumat ovat epätäydellisiä. Tällaisten jakaumien entropia voidaan määrittää luvussa 3.2.7 esiteltyyn yhtälöön 3.16 perustuen. Sovitettuna lähetetodennäköisyysjakaumalle, saadaan 1-asteen entropia nyt

$$H_1(P_r) = \frac{\sum_{i=1}^{S_r} p_i \log_2 \frac{1}{p_i}}{\sum_{i=1}^{S_r} p_i} \ . \qquad (4.3)$$

Määritelmänsä mukaisesti entropian avulla voidaan arvioida, miten paljon epävarmuutta joukon tai osajoukon tunnistamiseen liittyy. Mitä suurempi on osajoukon entropia, sitä vaikeammin se on lähetejakaumansa perusteella erotettavissa ympäristöstään. Laskettaessa entropia erikseen jokaiselle osajoukolle ja edelleen koko joukolle saadaan toistensa kanssa vertailukelpoiset lukuarvot, jotka antavat viitteitä kunkin osajoukon ja koko joukon tilastollisesta haavoittuvuudesta lähetetyyppien jakauman suhteen. On selkeästi havaittavissa, että entropia on sitä suurempi, mitä tasaisemmin osajoukon lähetetodennäköisyydet ovat jakautuneet. Tämä ominaisuus johtuu suoraan entropian määrittelyistä (ks. luku 3.2.2) ja on elektronisen suojautumisen kannalta tavoittelemisen arvoinen tilanne.

[10] Oletus on, että osajoukko ei sisällä kaikkia joukon lähettimiä. Jos sisältää, voi myös osajoukon painokerroin olla yksi.

Tarkasteltavassa tilanteessa on suuri kiusaus hyödyntää entropian yhteenlaskettavuutta siten, että alimman tason osajoukkojen oletetaan olevan toisistaan riippumattomia ja tällöin näitä ylempien osajoukkojen / joukon entropia muodostuisi suoraan alimman tason osajoukkojen entropioiden summana. Tällainen lähestymistapa on looginen ja perusteltu, mikäli mielenkiinnon kohteena on selvittää millainen osuus koko joukon sisältämästä informaatiosta sisältyy kuhunkin osajoukkoon. Tässä tarkastelussa ollaan kuitenkin kiinnostuneita lähetteiden tilastollisesta jakaumasta kullakin organisaatiotasolla erikseen. Näin ollen alimman tason osajoukot ovat itsenäisiä vain vertailtaessa niitä keskenään. Siirryttäessä ylemmälle tasolle oletetaan, että alemman tason lähetteet voivat ”sekoittua” keskenään ja näin ollen ne eivät enää ole toisistaan riippumattomia. Näin ollen entropian yhteenlaskettavuutta ei voida soveltaa, vaan entropia lasketaan erikseen jokaiselle eri tasolla olevalle osajoukolle ja koko joukolle.

Esimerkissä 4.1 on esitelty taulukkoa 4.1 soveltava joukko-lähete –taulukko ja sen pohjalta määritetyt lähetetodennäköisyydet, painokertoimet ja entropiat.

Esimerkki 4.1

Oletetaan, että erilaiset lähetteet tai lähettimet jakautuvat tarkasteltavassa joukossa taulukon 4.2 mukaisesti.

	L1	L2	L3	S_r
Joukko (JO0)	21	2	4	27
Osajoukko (OJ1.0)	5	0	3	8
- Osajoukko (OJ1.1)	3	0	2	5
- Osajoukko (OJ1.2)	2	0	1	3
Osajoukko (OJ2.0)	6	2	1	9
- Osajoukko (OJ2.1)	3	1	1	5
- Osajoukko (OJ2.2)	3	1	0	4
Osajoukko (OJ3.0)	10	0	0	10
- Osajoukko (OJ3.1)	5	0	0	5
- Osajoukko (OJ3.2)	5	0	0	5

Taulukko 4.2: Lähetekategorioihin L1, L2 ja L3 kuuluvien lähettimien jakautuminen joukon JO0 osajoukoille.

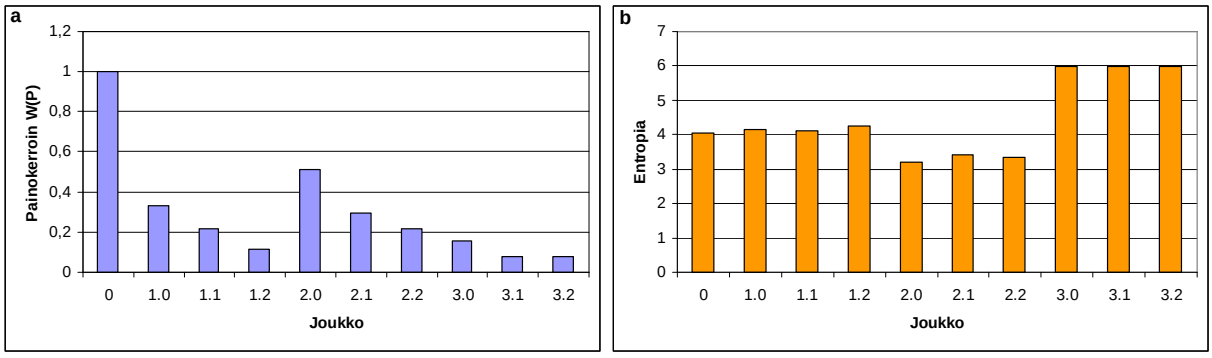
Satunnaisesti lähettimien L1 joukosta valitun lähetinyksilön todennäköisyys on 1/21. Vastaavat lukemat kategorioille L2 ja L3 ovat ½ ja ¼. Lähetekategorioiden lukumäärä on selvästi k = 3. Nyt lähetetodennäköisyydet voidaan määrittää yhtälön 4.1 mukaisesti ja ne ovat tässä tapauksessa: P_{L1} = 0.0159, P_{L2} = 0.1667 ja P_{L3} = 0.0833. Jokaiselle osajoukolle voidaan nyt muodostaa näihin lähetetodennäköisyyksiin perustuvat lähetetodennäköisyysjakaumat $P_r = (p_1, p_2, ..., p_{S_r})$. Esimerkiksi osajoukon OJ1.1 lähetetodennäköisyysjakauma on

$$P_{1.1} = (p_1 = 0.0159, p_2 = 0.0159, p_3 = 0.0159, p_4 = 0.0833, p_5 = 0.0833).$$

Lähetetodennäköisyysjakaumien perusteella voidaan laskea painokertoimet (yhtälö 4.2) ja entropiat (yhtälö 4.3) osajoukoille ja koko joukolle. Saadut tulokset on esitetty taulukossa 4.3. Tuloksia on havainnollistettu vielä kuvissa 4.3 a ja b.

	Painokerroin	Entropia
Joukko (JO0)	1	4.0514
Osajoukko (OJ1.0)	0.3294	4.1621
- Osajoukko (OJ1.1)	0.2143	4.1176
- Osajoukko (OJ1.2)	0.1151	4.2459
Osajoukko (OJ2.0)	0.5121	3.1935
- Osajoukko (OJ2.1)	0.2977	3.4081
- Osajoukko (OJ2.2)	0.2144	3.3391
Osajoukko (OJ3.0)	0.1590	5.9748
- Osajoukko (OJ3.1)	0.0795	5.9748
- Osajoukko (OJ3.2)	0.0795	5.9748

Taulukko 4.3: Joukon ja osajoukkojen painokertoimet ja entropiat.



Kuva 4.3: a) Jakaumien painokertoimet b) Entropiat ◇

Esimerkin tulosten perusteella voidaan havaita, että lähetetodennäköisyyksiin perustuvien todennäköisyysjakaumien muodostamat painokertoimet ilmaisevat varsin hyvin, mille osajoukoille todennäköisyysmassa on keskittynyt. Painokerroin ei kuitenkaan ilmaise välttämättä mitään siitä, miten tuo massa on jakautunut. Tästä saadaan käsitys entropian avulla, jonka voidaan ajatella kuvaavan tuon jakauman vaikeusastetta. Esimerkiksi osajoukkojen 1.1 ja 2.2 painokertoimet ovat lähes identtiset, mutta entropioissa on selkeä ero. Tämä johtuu todennäköisyysmassan keskittymisestä ”harvinaiselle” lähetteelle ja tätä kautta osajoukon 2.2 entropia (epävarmuus) on pienempi ja osajoukko on siis helpommin tunnistettavissa. Mielenkiintoinen yksityiskohta on myös osajoukko 3.0, johon kuuluu yli kolmannes koko joukon lähettimistä. Kuitenkin joukon entropia on hyvin suuri ja vieläpä sama kaikilla alijoukoilla. Tämä johtuu siitä, että todennäköisyysmassa on täysin tasajakautunut osajoukon 3.0 sisällä. Käytännössä

osajoukkojen 3.1 ja 3.2 painokertoimien ja entropioiden samanlaisuus kertoo, että osajoukkoja ei voi tilastollisesti erottaa toisistaan. Tämä ei kuitenkaan tarkoita sitä, että osajoukot 3.1 ja 3.2 olisivat välttämättä tunnistamattomia suhteessa koko joukkoon tai muihin osajoukkoihin, koska tunnistamisen voi perustaa myös sille mitä joukossa ei ole. Toisin sanoen, jotta yksikään osajoukko ei erottuisi toisistaan, tulisi kaikkien osajoukkojen entropioiden olla identtisiä.

Elektronisen suojautumisen kannalta entropia on ehkäpä painokerrointa tärkeämpi joukon / osajoukon tunnusluku. Todennäköisyysmassaa saattaa olla kertyneenä jollekin osajoukolle kohtuullisen paljonkin ja tämän perusteella osajoukkoa voitaisiin pitää erityisen kriittisenä tunnistamisen kannalta. Mikäli massa on kuitenkin jakautunut tasaisesti, on tyypillisesti myös entropia korkea ja tällöin osajoukko ei välttämättä ole erityisen haavoittuva tunnistamisen näkökulmasta. Optimaalisessa tilanteessa kaikkien osajoukkojen entropiat ovat samoja, jolloin eri osajoukkoja ei kyetä tilastollisesti erottamaan toisistaan.

Hyödyntämällä yllä esiteltyä menetelmää, voidaan erottaa erilaisten joukkojen elektronisen suojautumisen näkökulmasta kriittiset osajoukot. Kriittisten osajoukkojen olemassaolo on syytä tiedostaa joukkojen käyttöä suunniteltaessa tai esimerkiksi mahdollisissa kalustohankkeissa ja kehittämisessä.

4.2.3. Kriittisen toiminnan tunnistaminen

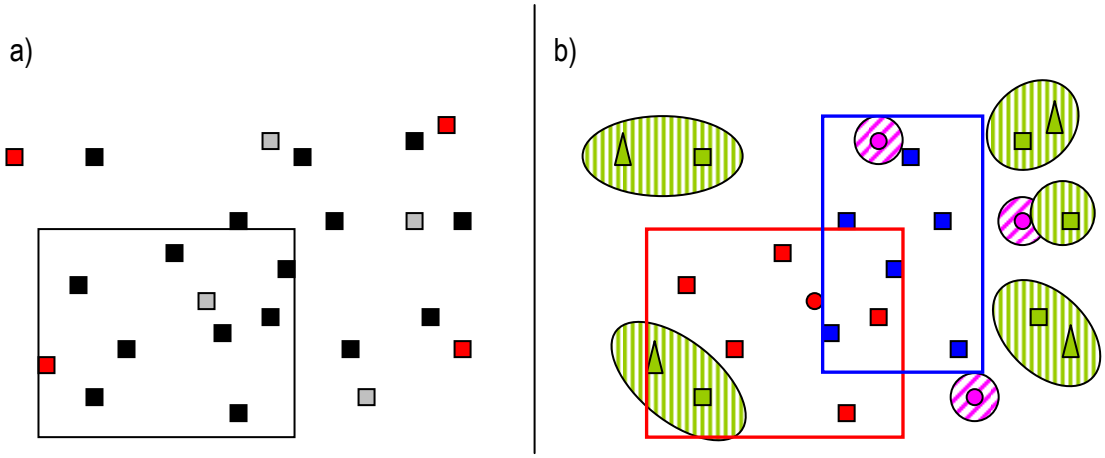
Kriittisellä toiminnalla ymmärretään mikä tahansa rajatun joukon toiminta, joka voi erityisesti olla tiedustelujärjestelmän mielenkiinnon kohteena. Rajatulla joukolla tarkoitetaan tässä, että kriittiselle toiminnalle voidaan määritellä seuraavia seikkoja:

- Mitkä organisaation osajoukot tai osajoukkojen osat osallistuvat ko. toimintaan? Tarvittaessa kriittiseen toimintaan voidaan määritellä osallistuvaksi lähettimiä useasta eri osajoukosta.
- Millainen on kriittiseen toimintaan liittyvä lähetekategoriajakauma ja kuinka paljon lähettimiä on?
- Millä alueella tai alueilla kriittinen toiminta toteutetaan ja milloin?

Tyypilliseen maakomponentin yhtymään sitoen, esimerkkeinä kriittisestä toiminnasta voisivat olla tiedustelutietojen välittäminen, esikuntien ja johtamispaikkojen ryhmitys, viestirunkoverkon rakenne, osaston hyökkäys tai siirto sekä tulenjohtoon liittyvä tiedonsiirto (vrt. esim. [39, s. 170]).

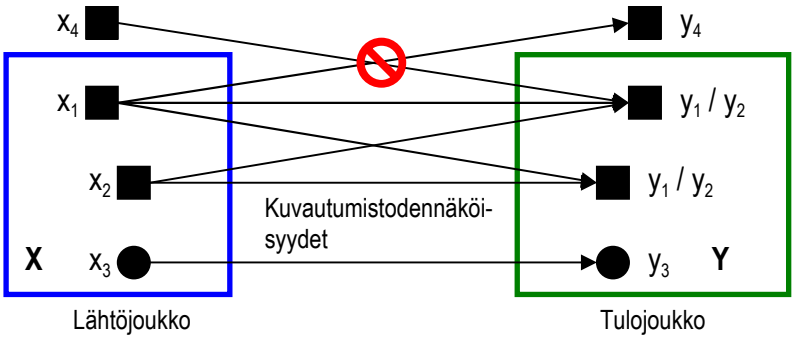
Kriittisiä toimintoja voi olla meneillään useita samanaikaisesti ja mahdollisesti myös maantieteellisesti limittyneinä toisiinsa. Lisäksi toimintaympäristössä saattaa olla toimijoita ja lähettimiä, joita ei sisällytetä mihinkään kriittiseen toimintaan. Pohjimmiltaan kriittisen toiminnan tunnistamisessa on siis kyse siitä, miten selkeästi tuohon toimintaan liittyvä lähetejakauma erottuu ympäristöstään (ks. kuva 4.4). Erottumisen kriteereinä ovat:

– Eri toimintojen maantieteellinen limittyneisyys.
– Samaan lähetekategoriaan kuuluvien lähettimien mahdollisuus sekoittua keskenään. Lähettimet voivat kuulua itse tarkasteltavaan toimintaan tai samalla alueella tapahtuvaan muuhun toimintaan.



Kuva 4.4: a) Kartta, jossa erityyppiset lähetteet tunnistettu (merkitty eri värein). Lähettimien liittymistä johonkin (kriittiseen) toimintaan ei kuitenkaan tiedetä. b) Kartta, johon erilaiset (kriittiset) toiminnat ja niihin liittyvät lähettimet tunnistettu. Esimerkissä neljä toimintoa: punainen, sininen, vihreä ja pinkki.

Käytännössä tarkastelussa tutkitaan, miten varmasti yksittäinen kriittiseen toimintaan kuuluvan lähetteen voidaan päätellä olevan juuri tämä tietty lähete. Samaan lähetinkategoriaan kuuluvat ja samalla maantieteellisellä alueella olevat muut lähettimet vaikeuttavat lähettimen identifiointia, koska tällöin on olemassa mahdollisuus, että lähettimet sekoittuvat toisiinsa eli ns. kuvautuvat ristiin. Kuvassa 4.5 on selvennetty tarkastelun problematiikkaa.

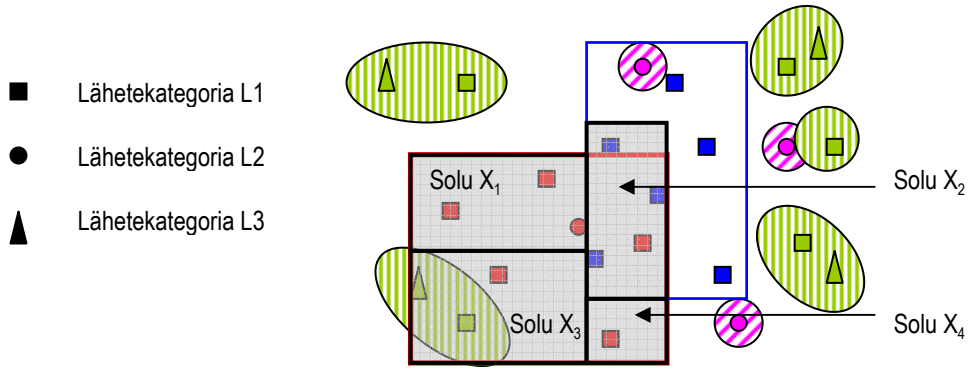


Kuva 4.5: Lähtöjoukko X kuvaa maantieteellisesti rajattua aluetta, jossa sijaitsevat lähettimet x_1, x_2 ja x_3. Näistä x_1 ja x_2 kuuluvat samaan lähetekategoriaan. Alueen X ulkopuolella sijaitsee lähetin x_4. Alueella X sijaitsevat samaan kategoriaan kuuluvat lähettimet voivat sekoittua keskenään eli kuvautua ristiin. Lähettimen x_3 kuvautuminen on yksikäsitteinen, koska samaan kategoriaan kuuluvia muita lähettimiä ei alueella ole. Kuvautuminen alueelta X tätä vastaavan alueen Y ulkopuolelle on kiellettyä. Samoin on kuvautuminen alueen X ulkopuolelta tulojoukkoon Y. Tulojoukko Y ilmentää alueen tilannetta, kun otetaan huomioon mahdolliset ristiinkuvautumiset.

Kriittisen toiminnan tunnistamista lähetejakaumaan ja lähetetodennäköisyyksiin perustuen voidaan tarkastella kolmessa eri mittakaavassa. Suuressa mittakaavassa yksittäiseen toimintaa liittyviä lähetteitä verrataan koko joukon lähetteisiin. Tällainen mittakaava saattaa johtaa varsin massiivisiin tarkasteluihin, mikäli aletaan arvioida yksittäisen lähettimen mahdollisuutta kuvautua miksi tahansa toiseksi samaan kategoriaan kuuluvaksi lähettimeksi. Tällaisen mittakaavan käsittely ei ole kannattavaa. Toisekseen suuren mittakaavan tarkastelu on tehty jo luvussa 4.2.2, jossa tarkasteltiin osajoukkojen entropioita osana koko joukkoa ja määritettiin lähetetodennäköisyydet kuvaamaan yksittäisen lähetteen yleisyyttä osana koko joukkoa. Pienen mittakaavan käsittelyssä voitaisiin rajata keskenään vertailtava lähettimet esimerkiksi paikannustarkkuuden mukaisesti. Tällöin kuitenkin tehdään oletus, että kriittisen toiminnan tunnistaminen on suoraan verrannollinen paikantamistarkkuuteen. Jos siis lähetin on paikannettu jollain tarkkuudella, niin tämän tarkkuuden ulkopuolelle jäävät samantyyppiset lähettimet eivät missään tilanteessa voi kuvautua ristiin. Tällainen mittakaava on varsin perusteltu etenkin tilanteessa, jossa voidaan paikantamistarkkuuden ajatella olevan erittäin hyvän ja tiedustelija on kyennyt rakentamaan tilannekuvaa jo jonkin aikaa[11]. Tarkastelun lähtökohdaksi voidaan kuitenkin ottaa mittakaava, joka on kooltaan keskisuuri. Lähtökohtaisesti rajataan tarkastelu koskettelemaan lähetteitä, jotka sijaitsevat kriittiselle toiminnalle määritetyllä alueella. Tarvittaessa alueiden kokoa voidaan edelleen supistaa jakamalla kriittiselle toiminnalle määritetty alue sopivan kokoisiin soluihin. Tämä voi olla tarpeen etenkin silloin, kun toiminnalle määritetty alue on laaja. Joissain tapauksissa saattaa olla tarpeen sisällyttää soluihin myös kriittiselle toiminnalle määritetyn alueen ulkopuolella olevia lähetteitä, mikäli ne ovat hyvin lähellä

[11] Eräs arvio on, että automatisoidulla tiedustelujärjestelmällä kyetään tuottamaan kohtuullisen hyvä pintatilannekuva alle kahdessa tunnissa tiheässäkin emissioympäristössä [39, s. 174].

tarkasteltavan toiminnan lähettimiä ja on siis vaara, että lähetteet kuvautuvat ristiin. Tarkastelu on sitä tarkempi, mitä pienempiin soluihin alue kyetään jakamaan. On kuitenkin huomattava, että rajoittumalla pienempiin soluihin, oletetaan aina, että vain solujen sisällä olevat lähetteet voivat kuvautua ristiin. Yhden solun sisällä oleva lähetin ei saa koskaan kuvautua solun ulkopuolelle, koska solujen tulee olla täysin riippumattomia toisistaan. Tätä ehtoa noudattamalla voidaan erillisten solujen sisältämät informaatiot laskea sellaisenaan yhteen ja lopputulokseksi saadaan koko kriittisen toiminnan tunnistettavuutta kuvaava lukema. Esimerkki kriittiselle toiminnalle määritellyn alueen jakamisesta soluihin on kuvassa 4.6.



Kuva 4.6: Esimerkki, jossa tarkastelun kohteena punaisella merkitty kriittinen toiminta / osajoukko (X_0). Alue jaettu tarkastelua varten neljään pienempää soluun (X_1, X_2, X_3 ja X_4).

Informaatioteoreettinen analyysi perustuu luvussa 3.2.8 esitellyn yhtenäisinformaation hyödyntämiseen. Käytännössä tarkastelu sisältää seuraavat vaiheet:

- Jokaiselle solulle ja koko tarkasteltavalle alueelle lasketaan entropia lähetetodennäköisyyksiin perustuen.
- Jokaiselle solulle määritetään kuvautumistodennäköisyydet eli tarkastellaan, mitkä solun sisältämät lähettimet voivat kuvautua ristiin.
- Määritetään vastaanottotodennäköisyydet kaikille soluille ja tämän perusteella voidaan laskea tulojoukon entropia.
- Lasketaan vielä yhteinen todennäköisyysjakauma $p(\cdot,\cdot)$, ja tämän perusteella voidaan laskea yhteinen lähtö- ja tulojoukon yhteinen entropia.
- Lasketaan yhtenäisinformaatio jokaiselle solulle. Yhteisinformaatio kertoo, kuinka paljon solun informaatiosta on pääteltävissä pelkästään tuntemalla tulojoukko. Koko kriittiselle toiminnalle määritetyn alueen yhteisinformaatio saadaan laskemalla yhteen erillisten solujen yhteisinformaatiot.
- Verrataan solujen ja koko alueen alkuperäistä entropiaa laskettuihin yhtenäisinformaatioihin. Vertailun avulla on pääteltävissä, millaisella varmuudella kunkin solun ja koko

alueen lähettimet ovat tunnistettavissa kuuluviksi mielenkiinnon kohteena olevaan toimintaa tai osajoukkoon.

Seuraavassa oletetaan, että mielenkiinnon kohteena olevalla alueella on joukko lähettimiä. Tämä joukko määritellään $X_0 = \{x_1, x_2, ..., x_m\}$. Alue X_0 on jaettu soluihin X_k (k = 1, …, N) siten, että $\bigcap_{k=1}^{N} X_k = \varnothing$ ja $\bigcup_{k=1}^{N} X_k = X_0$. Lähettimet x_i ovat jakaantuneet näennäisen satunnaisesti eri soluihin kuitenkin siten, että kaikissa soluissa on ainakin yksi lähetin eli $X_k \neq \varnothing \ \forall k$. Jokaista lähetintä vastaa määritelmän 4.1 mukainen lähetetodennäköisyys. Näin ollen saadaan muodostettua lähetetodennäköisyysjakaumat jokaiselle solulle. Jakaumat ovat muotoa $P_L(X_k) = \left(p(x_g), ..., p(x_h)\right)$, missä $g, h \in \{1, ..., m\}$ ja $g < h$. Toisistaan riippumattomat lähetetodennäköisyysjakaumat voidaan muodostaa kaikille soluille X_k niihin sisältyvien lähettimien mukaisesti. Nämä lähetetodennäköisyysjakaumat ovat tyypillisesti epätäydellisiä ja tällöin kunkin solun entropia voidaan laskea yhtälön 3.16 avulla. Solujen riippumattomuus toisistaan takaa sen, että koko alueen entropia saadaan solujen entropioiden summana (entropian yhteenlaskettavuus, ks. luku 3.2.2)

$$H_1(X_0) = \sum_{k=1}^{N} H_1(X_k). \qquad (4.4)$$

Erilliset solut X_k toimivat lähtöjoukkoina (ks. luku 4.1.2) tarkasteltaessa seuraavaksi kunkin solun erottuvuutta ympäristöstään. Tulojoukkona toimivat solut Y_k, jossa k = 1, …, N. Lisäksi vaaditaan, että lähtöjoukon symboli (lähetin) voi kuvautua vain ja ainoastaan tätä solua vastaavaan tulojoukkoon eli $x_i \in X_r \subset X_0 \mapsto y_j \in Y_s \subset Y_0$, missä $r = s$.

Kuvautumistodennäköisyyksillä säädellään sitä, miten lähtöjoukon symbolit (lähettimet) kuvautuvat tulojoukkoon. Yllä oletettiin, että symboli ei saa kuvautua solunsa ulkopuolelle. Lisäksi oletetaan, että vain samaan lähetekategoriaan kuuluvat lähettimet voivat kuvautua ristiin (sekoittua toisiinsa) ja todennäköisyys kuvautua johonkin toiseen kategoriaan on nolla. Tässä tarkastelussa keskitytään vain lähetejakaumien tarkasteluun ja näin ollen kuvautumistodennäköisyyksissä ei huomioida mitään fysikaalisia ja teknisiä häiriöitä. Näiden tarkastelujen vuoro on luvussa 4.3. Näiden oletusten vallitessa kuvautumistodennäköisyydet määräytyvät yhden solun osalta seuraavasti:

$$c_{ij} = \begin{cases} \frac{1}{S^{Ln}} & \text{, kun } x_i \in Lr \text{ ja } y_j \in Ls \text{ ja } r = s \\ 0 & \text{, kun } x_i \in Lr \text{ ja } y_j \in Ls \text{ ja } r \neq s \end{cases} \quad i \in \{g,...,h\} \text{ja } \; j \in \{g,...,h\}, \qquad (4.5)$$

missä S^{Ln} = solussa olevien samaan lähetekategoriaan kuuluvien symbolien lukumäärä

Ln on lähetekategorian tunnus.

Toisin sanoen lähtöjoukon symboli kuvautuu yhtä suurella todennäköisyydellä miksi tahansa tulojoukon symboliksi, jos tämä kuuluu samaan lähetekategoriaan. Kuvautuminen toiseen lähetekategoriaan ei ole mahdollista.

Yhtenäisinformaatio voidaan laskea kullekin solulle yhtälöllä (ks. luku 3.2.8)

$$I(X_k;Y_k) = H(X_k) + H(Y_k) - H(X_k,Y_k), \qquad (4.6)$$

missä X_k = lähetetodennäköisyyksiin perustuva lähtöjoukko,

Y_k = vastaanottotodennäköisyyksiin perustuva tulojoukko.

Kuten todettua, on solua X_k vastaava lähetetodennäköisyysjakauma epätäydellinen. Voidaan osoittaa, että jos lähtöjoukon todennäköisyysjakauma on epätäydellinen, niin tällöin myös tulojoukon solua Y_k vastaava vastaanottotodennäköisyysjakauma sekä näiden kahden yhteinen todennäköisyysjakauma ovat epätäydellisiä. (ks. liite 1). Tällöin yhtenäisinformaatio määritetään muodossa

$$I(X_k;Y_k) = H_1(X_k) + H_1(Y_k) - H_1(H_k,Y_k). \qquad (4.7)$$

Lisäksi voidaan osoittaa, että jos vain samaan lähetekategoriaan kuuluvat symbolit voivat kuvautua ristiin, niin tällöin lähetetodennäköisyysjakauma on täysin sama kuin vastaanottotodennäköisyysjakauma (ks. liite 1). Kahden täysin samanlaisen diskreetin todennäköisyysjakauman entropiat ovat samansuuruiset. Näin ollen lauseke 4.7 voidaan lausua

$$I(X_k;Y_k) = 2H_1(X_k) - H_1(X_k,Y_k). \qquad (4.8)$$

Yhteisentropia on yleisesti määritelty [62, s. 12], [16, s. 16]:

$$H(X,Y) = \sum_{i,j} p(x_i,y_j) \log_2 \frac{1}{p(x_i,y_j)}. \qquad (4.9)$$

Sovitettuna yhden solun tarkasteluun ja epätäydelliselle todennäköisyysjakaumalle, yhteisentropia voidaan lausua

$$H_1(X_k, Y_k) = \frac{\sum_{i=g}^{h}\sum_{j=g}^{h} p(x_i, y_j)\log_2 \frac{1}{p(x_i, y_j)}}{\sum_{i=g}^{h}\sum_{j=g}^{h} p(x_i, y_j)}, \qquad g, h \in \{1, ..., m\}. \tag{4.10}$$

Yhtälö 4.8 voidaan nyt lausua muodossa (ks. myös liite 1)

$$I(X_k; Y_k) = \frac{1}{W(P_L)}\left[2\sum_{i=g}^{h} p(x_i)\log_2 \frac{1}{p(x_i)} - \sum_{i=g}^{h}\sum_{j=g}^{h} p(x_i, y_j)\log_2 \frac{1}{p(x_i, y_j)}\right], \tag{4.11}$$

missä $W(P_L) = \sum_{i=g}^{h} p(x_i)$ eli lähtöjoukon painokerroin (ks. luku 3.2.7).

Mikäli solut ovat täysin riippumattomia toisistaan, voidaan minkä tahansa kahdesta tai useammasta solusta muodostuvan alueen yhtenäisinformaatio laskea erillisten solujen yhtenäisinformaatioiden summana. Tämä johtuu informaation yhteenlaskettavuudesta ja on myös osoitettu liitteessä 1. Näin ollen voidaan lausua

$$I(X_0; Y_0) = I(X_1; Y_1) + ... + I(X_N; Y_N) = \sum_{k=1}^{N} I(X_k; Y_k), \tag{4.12}$$

missä $X_1, ..., X_N \subset X_0$ ja $Y_1, ..., Y_N \subset Y_0$.

Soluille ja koko alueelle voidaan laskea entropioiden ja yhtenäisinformaatioiden erotus, joka kertoo millainen määrä alkuperäisestä solun tai alueen informaatiosta jää vähintään epäselväksi (vrt. [10] ja [40, s. 156] määritelmät). Mitä suurempi erotus on, sitä epäselvempi solun tai alueen tilanne on. Kuten yhtälöstä 3.17 on pääteltävissä, entropian ja yhtenäisinformaation erotus on ehdollinen entropia $H(\cdot \mid \cdot)$ eli

$$H(X_k \mid Y_k) = H(X_k) - I(X_k; Y_k), \tag{4.13}$$

missä $k = 0$ kun kyseessä on koko alue

$k = 1, \ldots, N$ kun kyseessä ovat erilliset solut.

Yhtenäisinformaation suhteellinen osuus entropiasta voidaan tulkita varmuudeksi, jolla solun tai alueen lähettimet kyetään yksilöimään ja tätä kautta mahdollisesti tunnistamaan kuuluvaksi mielenkiinnon kohteena olevaan kriittiseen toimintaan tai osajoukkoon. Suhde määritetään

$$\frac{I(X_k;Y_k)}{H(X_k)} \leq 1, \qquad k = 0, \ldots, N. \tag{4.14}$$

Suhde 4.14 on yksi vain, jos kaikkien tarkasteltavan solun tai alueen lähettimet kuvautuvat yksikäsitteisesti (ovat identifioitavissa).

On muistettava, että tässä esitelty menetelmä ei suoranaisesti kerro esimerkiksi todennäköisyyttä, jolla jokin kriittinen toiminta tunnistetaan tai erotetaan ympäristöstään. Pikemminkin menetelmä kuvaa vaikeusasteen, jolla jokin toiminta on hahmotettavissa tietyltä alueelta ja pelkästään lähetekategorioihin perustuen.

Esimerkki 4.2

Esimerkin laskutoimitukset ja välivaiheet on esitelty tarkemmin liitteessä 2.

Olkoon tarkasteltava tilanne kuvan 4.5 mukainen. Oletetaan, että lähetekategoriaa L1 vastaa lähetetodennäköisyys P_{L1} = 0.0159, kategoriaa L2 vastaa P_{L2} = 0.1667 ja kategoriaa L3 vastaa P_{L3} = 0.0833 (lähetetodennäköisyydet esimerkin 4.1 mukaiset). Lähettimet ovat jakautuneet soluihin seuraavasti:

$$X_1 = \left\{x_1^{L1}, x_2^{L1}, x_3^{L2}\right\}$$
$$X_2 = \left\{x_4^{L1}, x_5^{L1}, x_6^{L1}, x_7^{L1}\right\}$$
$$X_3 = \left\{x_8^{L1}, x_9^{L1}, x_{10}^{L3}\right\}$$
$$X_4 = \left\{x_{11}^{L1}\right\}$$

Kun on laskettu entropia ja yhtenäisinformaatio kullekin solulle ja koko alueelle, lopputulokseksi saadaan taulukko 4.4.

	Entropia H	Yhtenäisin-formaatio I	Erotus (H-I)	Prosenttia I/H
Solu 1	3.1278	2.9676	0.1602	94.9 %
Solu 2	5.9748	3.9666	2.0082	66.4 %
Solu 3	4.2457	3.9694	0.2763	93.5 %
Solu 4	5.9748	5.9748	0	100 %
Koko alue	19.3231	16.8784	2.4447	87.3 %

Taulukko 4.4: Yhteenveto esimerkkitilanteen 4.2 tuloksista.

Havaitaan, että solu 2 on ”epäselvin” ja symboleiden mahdollinen kuvautuminen ristiin aiheuttaa sen, että lähetinten yksilöinti juuri tietyksi lähettimeksi on mahdollista vain noin 66 prosentin varmuudella. Solun numero 4 lähetin kyetään luonnollisesti yksilöimään 100 % varmuudella. Myös solut 1 ja 3 ovat varsin selkeitä. Kaiken kaikkiaan koko alueen sisältämästä informaatiosta (n. 19.3 bittiä) jää epäselväksi vähintään noin 2.4 bittiä eli noin 13 %. Loppujen lopuksi tilanne on siis kohtuullisen selkeä ja mahdollisuudet mielenkiinnon kohteena olleen toiminnan tai osajoukon tunnistamiselle ovat olemassa. Voidaan todeta, että intuitiivisesti tämä ei näin selvästi ole havaittavissa esimerkiksi kuvista 4.4 a ja b.

◇

Esimerkki 4.3

Tarkastellaan vastaavaa tilannetta kuin yllä, mutta oletetaan, että kaikki mielenkiinnon kohteena olevan alueen lähettimet kuuluvat samaan lähetekategoriaan (L1). Tulokset ovat taulukossa 4.5 esitetynlaisia.

	Entropia H	Yhtenäisinformaatio I	Erotus (H-I)	Prosenttia I/H
Solu 1	5.9748	4.4476	1.5272	74.4 %
Solu 2	5.9748	3.9666	2.0082	66.4 %
Solu 3	5.9748	4.4476	1.5272	74.4 %
Solu 4	5.9748	5.9748	0	100 %
Koko alue	23.8992	18.8366	5.0626	78.8 %

Taulukko 4.5: Yhteenveto esimerkkitilanteen 4.3 tuloksista.

Tuloksista havaitaan, että solujen 1 ja 3 suhteellinen varmuus on tipahtanut huomattavasti verrattuna esimerkkiin 4.2. Tämä on suora tulos ”harvinaisten” lähetekategorioiden L2 ja L3 poistumisesta emissioympäristöstä. Toisin sanoen yksittäiset lähetteet, jotka poikkeavat selkeästi ympäristöstään, tuottavat huomattavan määrän informaatiota kriittisen toiminnan tai osajoukon tunnistamiseksi. ◇

Yllä olevasta esimerkistä havaitaan myös, että solujen entropiat ovat identtiset, mikäli kaikki lähettimet kuuluvat samaan lähetekategoriaan. Tämä perustuu suoraan tasajakautuneen todennäköisyysmassafunktion entropian ominaisuuksiin (ks. luku 3.2.2), joista mm. johtuu, että tällöin entropian määrä on suurin mahdollinen. Tässä luvussa esitellyt menetelmät käsittelevät kuitenkin epätäydellisiä todennäköisyysjakaumia, jolloin täydelliselle jakaumalle esitellyt laskentasäännöt eivät sellaisenaan täysin päde. Voidaan osoittaa (ks**.** liite 1), että epätäydelliselle tasajakaumalle ensimmäisen asteen entropia lasketaan

$$H_1 = \log_2 \frac{1}{P_L}, \qquad (4.15)$$

missä P_L = tapahtuman todennäköisyys, joka tässä tapauksessa on lähetekategoriaa vastaava lähetetodennäköisyys.

4.3. Osajoukon aktiivisuuden arviointi entropiaan ja yhtenäisinformaatioon perustuen

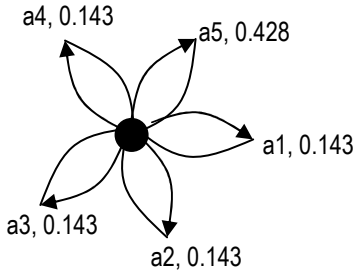
4.3.1. Emissiomalli

Emissiomallilla kuvataan, miten erilaisia joukon ja/tai sen osajoukon lähettimiä käytetään. Tämän työn näkökulmana emissiomallin rakenteelle on luvussa 3.2.3 esitelty diskreetti informaation lähde, jolloin mallia arvioitaessa ja hyödynnettäessä käytössä ovat informaatioteorian mukaiset työkalut. Luvussa 3.2.3 on kuvattu diskreetti informaation lähde Markovin ketjuksi, jolla on ergodiset ja vakaat ominaisuudet.

Suurehko sotilasorganisaatio saattaa sisältää useita erilaisia lähetetyyppejä, mahdollisesti jopa satoja lähettimiä ja kymmeniä erilaisia verkkoja [53, s. 444] ja [58, s. 87 - 107]. Tällaisen joukon emissiomallin rakentaminen yhdeksi suureksi Markov ketjuksi on käytännössä mahdotonta. Miten esimerkiksi voitaisiin kuvata samaan prosessiin jokin alhaisella toimintasuhteella toimiva kenttäradio ja koko ajan lähettävä linkkiradio tai vaikkapa tutkalähetin? Väistämättä törmätään ongelmiin, jotka vääristävät mallia liiaksi suhteessa todellisuuteen tai ainakin rikotaan vaatimuksia, joita diskreetille informaation lähteelle on edellä asetettu. Emissiomalli onkin syytä määritellä sopiviin osiin jaettuina rinnakkaisina prosesseina. Jako voidaan tehdä esimerkiksi organisaation mukaisiin osajoukkoihin perustuen, järjestelmittäin, johonkin kriittiseen toimintaan perustuen tai radioverkkorakenteeseen pohjautuen. Rinnakkaiset prosessit mahdollistavat myös samaan aikaan tapahtuvien ja toisistaan riippumattomien toimintojen kuvaamisen, joka on varsin tyypillistä suurelle joukkokokonaisuudelle.

Emissiomallia varten jokainen organisaation lähetin merkitään symbolilla, esimerkiksi a_1 … a_n. Jokaista symbolia kohden asetetaan todennäköisyys p_1 … p_n, joka kuvastaa tuon symbolin tilastollista yleisyyttä prosessissa. Kun Markov ketju tuottaa jonkin symbolin a_k tämä tarkoittaa, että lähetin a_k on ollut aktiivinen ja tuottanut informaatiota sähkömagneettiseen spektriin.

Markov ketjuun perustuva emissiomalli on ehkäpä luonnollisinta mieltää kuvaamaan erilaisten radioverkkojen toimintaa. Yksinkertaisimmillaan radioverkon liikennöintimalli kuvaa vain kunkin lähettimen (symbolin) suhteellista aktiivisuutta verrattuna verkon muihin lähettimiin (symboleihin). Jos oletetaan, että peräkkäisten symboleiden järjestystä ei rajoiteta millään tavalla, ovat peräkkäiset tapahtumat toisistaan riippumattomia ja lopputuloksena on prosessi jolla on vain yksi tila (vrt. luvut 3.2.3 ja 3.3.1). Oletetaan esimerkiksi, että radioverkossa on viisi lähetintä, joita merkitään symboleilla $a_1 - a_5$. Kaikki lähettimet ovat yhtä aktiivisia paitsi lähetin a_5, joka on noin kolme kertaa aktiivisempi, kuin yksikään muista lähettimistä. Kuvassa 4.7 on esitetty kaavio esimerkin prosessista todennäköisyysjakaumineen.

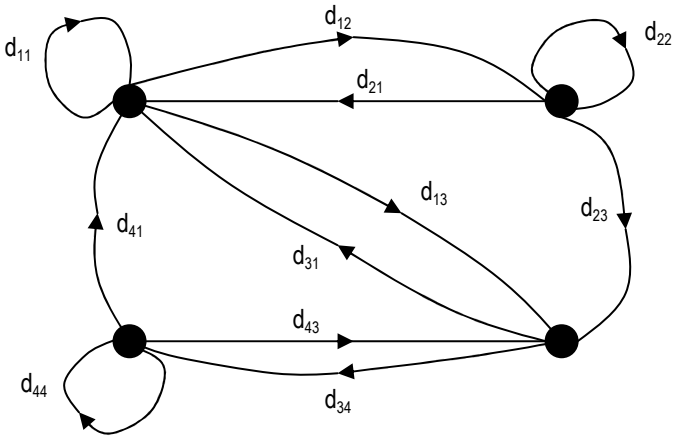


Kuva 4.7: Yksinkertainen radioverkon emissiomalli.

Mikäli emissiomallissa kuvataan myös peräkkäisten symbolien riippuvuuksia toisistaan, on tuloksena Markov ketju, jossa on yhtä monta tilaa kuin on lähettimiä radioverkossa. Lähettimet merkitään esimerkiksi symboleilla d_{ij}, jossa d_i identifioi varsinaisesti lähettimen ja j kertoo mihin tilaan ollaan siirtymässä. Jokaista symbolia d_{ij} vastaa siirtymätodennäköisyys P_{ij}.

Esimerkki 4.4

Oletetaan, että radioverkossa on neljä lähetintä $d_1 - d_4$ ja että kaavio emissiomallista on kuvan 4.8 mukainen.



Kuva 4.8: Emissiomalli, jossa peräkkäisten symbolien valinta riippuu edellisestä symbolista. Nuolet kuvaavat tuotettuja symboleita ja siirtymiä tilojen välillä. Prosessin tiloja kuvaavat siirtymänuolien risteykset.

Jokaista symbolia ja siirtymää vastaa siirtymätodennäköisyys alla olevan matriisin mukaisesti.

$$\begin{pmatrix} d_{11} & d_{12} & d_{13} & d_{14} \\ d_{21} & d_{22} & d_{23} & d_{24} \\ d_{31} & d_{32} & d_{33} & d_{34} \\ d_{41} & d_{42} & d_{43} & d_{44} \end{pmatrix} \quad \Rightarrow \quad \mathrm{P} = \begin{pmatrix} P_{11} & P_{12} & P_{13} & P_{14} \\ P_{21} & P_{22} & P_{23} & P_{24} \\ P_{31} & P_{32} & P_{33} & P_{34} \\ P_{41} & P_{42} & P_{43} & P_{44} \end{pmatrix} \tag{4.16}$$

Esimerkiksi oltaessa tilassa 1 tuotetaan symboli d_1 ja palataan tilaan 1 todennäköisyydellä P_{11}. Edelleen todennäköisyydellä P_{12} tuotetaan symboli d_1 ja siirrytään tilaan 2. Tilaan 3 siirrytään tilasta 1 todennäköisyydellä P_{13}. Tilaan 4 siirtyminen ei tilasta 1 ole mahdollista ($P_{14} = 0$) eli toisin sanoen symbolin d_1 jälkeen ei voi tulla symbolia d_4.

Tarkasteltaessa tilaa 3 havaitaan, että symbolin d_3 jälkeen voi tulla jompikumpi symboleista d_1 tai d_4. Siirtyminen takaisin tilaan 3 tai tilaan 2 ei emissiomallin mukaan ole sallittua eli symboli d_3 ei voi esiintyä kahta kertaa peräkkäin eikä symboli d_2 voi seurata symbolia d_3. ◇

Kuten yllä olevasta esimerkistä huomataan, voidaan tämän tyyppisellä mallinnuksella säädellä sitä, millaisia keskinäisriippuvuuksia lähettimillä tilastollisesti on. On huomattava, että emissiomalli määrittelee nimensä mukaisesti vain eri lähetinyksilöiden aktiviteettia eli sitä, miten emissioympäristö tilastollisesti tuottaa informaatiota sähkömagneettiseen spektriin. Malli ei varsinaisesti ota mitään kantaa siihen, kelle tuo aktiivisuus on suunnattu tai mitä informaatio sisältää. Yksittäinen lähete (symboli) voi olla tarkoitettu yhdelle tai useammalle vastaanottajalle. Toki mallinnukseen voi vaikuttaa suurestikin se, millainen organisaation viestiliikennekulttuuri on. Esimerkiksi hyvin hierarkkisessa kulttuurissa johtoasema saattaa lähettää varsin usein erikseen jokaiselle ala-asemalleen. Ala-asemat ehkäpä varmistavat johtoaseman lähetteet vastaanotetuiksi ja näin ollen liikennöivät silloin tällöin johtoaseman suuntaan, kun taas liikennöinti suoraan ala-asemien välillä on hyvin vähäistä. Muodostettaessa todennäköisyyksiin pohjautuvaa prosessia tästä emissioympäristöstä, korostunee johtoaseman symbolin esiintyminen varsin usein peräkkäin ja suurella todennäköisyydellä aina myös ala-asemien symboleiden välissä. Sen sijaan voidaan arvioida, että ala-asemien symbolit ovat peräkkäin vain hyvin pienellä todennäköisyydellä, jos ollenkaan.

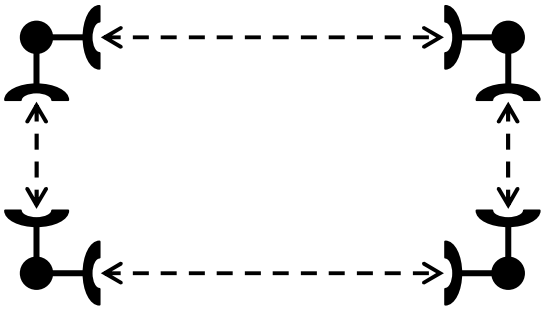
Myöhemmin tullaan havaitsemaan, että emissiomallin hyödyntäminen on monella tapaa mahdollista, vaikka sitä ei sidottaisikaan aikaan, vaan tarkastellaan vain keskimääräistä entropiaa per symboli. Joissain tarkasteluissa on kuitenkin ensiarvoisen tärkeää, että emissiomalli kyetään sitomaan myös aikaan. Näin on, jos mallin avulla halutaan arvioida emissioympäristön tuottaman informaation määrää jonkin aikaikkunan puitteissa. Tätä varten jokaiselle prosessin

tilalle on määriteltävä nopeus, joka ilmaisee, kuinka monta symbolia tila keskimäärin tuottaa aikayksikössä. Toisin sanoen tilan symbolinopeus (φ_i) kertoo, kuinka nopeasti tila keskimäärin tuottaa symbolin prosessin saapuessa tähän tilaan. Symbolinopeuden yksikkö on tyypillisesti symbolia per sekunti ja se voidaan merkitä:

$$\varphi_i = \begin{pmatrix} \varphi_1 \\ \varphi_2 \\ \vdots \\ \varphi_n \end{pmatrix}, \quad \text{missä } n \text{ on prosessin tilojen lukumäärä.} \qquad (4.17)$$

Mallista puuttuu vielä määritelmä symbolien ajallisille pituuksille. Voitaisiin esimerkiksi määrittää, että kussakin tilassa muodostetun symbolin pituus noudattelee normaalijakaumaa jollain tilalle tyypillisellä odotusarvolla ja poikkeamalla. Symbolin (lähetteen) pituudella voi olla merkitystä esimerkiksi signaalin havaitsemisen kannalta [53, s. 461 - 464] ja [67, s. 301 - 302]. Symbolin pituudella ei kuitenkaan ole merkitystä tässä esitetyn emissiomallin näkökulman kannalta. Tilastollinen kokonaiskuva emissioympäristöstä luodaan diskreetin informaation lähteen tuottamien symboleiden jakauman kautta. Symbolien pituudet eivät tähän jakaumaan vaikuta. Tarvittaessa voidaan olettaa, että symbolit ovat riittävän pitkiä, jotta ne voidaan hyödyntää muodostettaessa elektronista tilannekuvaa ympäristöstä.

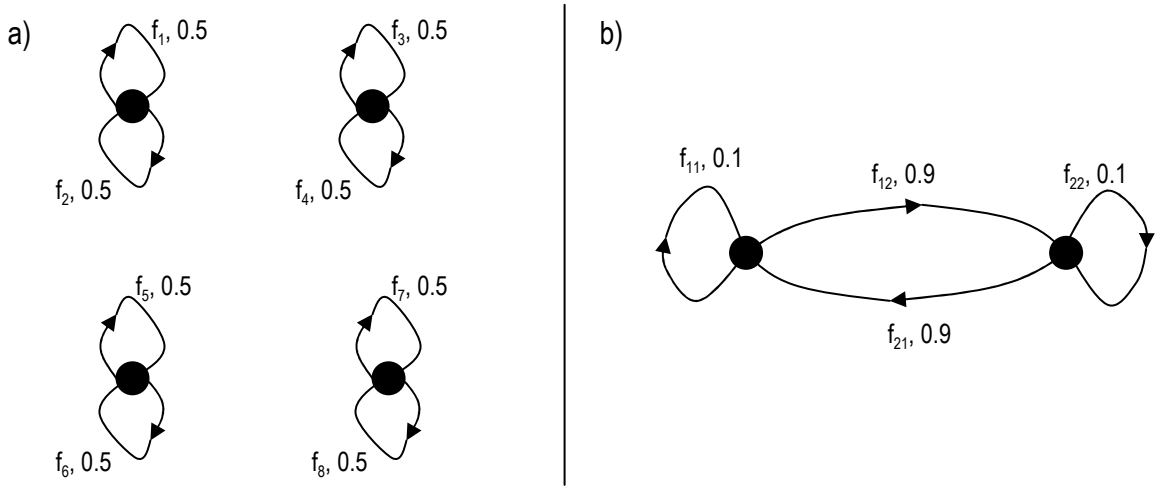
Tyypillisesti esimerkiksi maakomponentin taktisen tason yhtymien tiedonsiirtoyhteydet perustuvat ns. runkoverkkoon, joissa siirtotiet toteutetaan suurelta osin radiolinkeillä [33, s. 171] ja [58, s. 187 - 204]. Seuraavassa hahmotellaan, miten radiolinkkeihin perustuva verkko voidaan kuvata diskreettinä informaation lähteenä. Mallinnus on väistämättä hieman keinotekoinen johtuen radiolinkeillä toteutettujen yhteyksien ominaisuuksista. Linkkijänne muodostetaan kahden radiolinkin välille siten, että kummatkin lähettävät jatkuvasti eri taajuuksilla ja vastaavasti vastaanottavat vasta-asemansa signaalia tämän lähetystaajuudella [31, s. 16 ja 20]. Näin ollen voitaisiin ajatella, että radiolinkin tuottaman symbolin (lähetteen) pituus on ääretön tai ainakin niin pitkä, kuin radiolinkki on toiminnassa. Toisaalta voidaan myös ajatella, että radiolinkki tuottaisi symboleita äärettömän suurella symbolinopeudella. Tarkastellaan tilannetta kuvassa 4.9 esitetyn linkkikaavion esimerkin valossa.



Kuva 4.9: Radiolinkkiverkko, jossa kahdeksan radiolinkkiä ja neljä linkkijännettä.

Kuvan 4.9 mukaisessa tilanteessa emissioympäristö voitaisiin kuvata siten, että jokainen kahden radiolinkin muodostama ”asema” kuvataan erillisiksi ja toisistaan riippumattomiksi prosesseiksi, joissa kumpaakin symbolia tuotetaan todennäköisyydellä 0.5 (ks. kuva 4.10 a). Jos symbolinopeus asetetaan hyvin suureksi, voidaan mieltää, että tilanne mallintaisi radiolinkkiverkkoa riittävästi. Symboleiden todennäköisyysjakaumat on pidettävä tasajakautuneina, jotta yksikään symboli ei tilastollisesti ylikorostu.

Toinen, ja ehkäpä luonnollisempi, tapa kuvata radiolinkkiverkko on tarkastelu linkkijänteittäin. Tällöin saadaan muodostettua kaksitilainen Markov ketju kuvan 4.10 b mukaisesti. Asettamalla siirtymätodennäköisyydet tilasta toiseen suuriksi verrattuna tiloihin palaaviin todennäköisyyksiin, voidaan saavuttaa tilanne, jossa kumpaakin radiolinkkiä kuvaavia symboleita muodostuu tilastollisesti hyvin tasaisesti.



Kuva 4.10: a) Radiolinkkiverkko kuvattuna ”asemittain”. b) Linkkijänne kuvattuna kaksi tilaa omaavana Markov ketjuna. Piirroksessa esitetty vain yksi jänne. Siirtymätodennäköisyyksiä tilojen välillä on painotettu suhteessa lähtötilaansa palaaviin siirtymiin.

Tässä luvussa esitetyllä tavalla voidaan kuvata joukon tilastollista aktiivisuutta sähkömagneettisen spektrin osalta. Voidaan mieltää, että emissiomalli toimii koko emissioympäristön lähettimenä ja toimittaa emissioympäristön haluaman informaation kanavalle (vrt. kuva 4.1). Koska suuren joukon aktiivisuuden kuvaaminen kokonaisuutena on vaikeaa, eikä välttämättä edes tarpeellista, on joukko jaettava sopiviin osajoukkoihin siten, että tilastollinen kuvaaminen on

kohtuullisella tarkkuudella mahdollista. Jos lopullisena tavoitteena on vertailla joukon tai osajoukon elektronista aktiivisuutta olosuhteiden A ja B välillä, niin tällöin mallille voidaan suoda epätarkkuuksia. Mallilla ja siihen liittyvällä analyysilla on kuitenkin saavutettava tilanne, jossa kyetään esimerkiksi toteamaan, että joukko tuottaa informaatiota tiedustelijan käytettäväksi enemmän olosuhteiden A vallitessa verrattuna olosuhteisiin B. Jos vielä kyetään edes karkeasti määrittämään, kuinka paljon enemmän tuota informaatiota on käytettävissä, niin tällöin erilaisten elektronisen suojautumisen toimenpiteiden ja taktisten ratkaisujen vertailu on jo mahdollista.

4.3.2. Emissiomallin entropian määrittäminen

Emissiomallin entropia kertoo, kuinka paljon informaatiota ko. malli toimittaa siirtotielle eli sähkömagneettiseen spektriin (vrt. kuva 4.1). Entropian voidaan katsoa ilmaisevan pienimmän keskimääräisen ”kyllä / ei” kysymysten määrän, joka tarvitaan yksittäisen lähteessä tuotetun symbolin identiteetin selvittämiseksi [4, s. 12 – 14]. Voidaan siis todeta, että mitä suurempi emissiomallin entropia on, sitä monimutkaisemmasta tilanteesta on kyse. Elektronisen suojautumisen näkökulmasta tilanne on hieman ristiriitainen, koska yleensä sähkömagneettiseen spektriin pyritään tuottamaan mahdollisimman vähän tiedusteltavaa dataa. Emissiomallin tuottama informaatio on kuitenkin ymmärrettävä informaatioteoreettisesta näkökulmasta, jolloin se voidaan mieltää epävarmuudeksi kokeilun tuloksesta, ennen kuin tuo todennäköisyyksiin perustuva kokeilu on toteutettu (ks. [55]).

Emissiomallille on syytä määrittää lähtökohtaolosuhteet (ns. perusasetukset), jotka kuvaavat tuotetun informaation määrää tietyissä kiinnitetyissä olosuhteissa. Lähtökohtaolosuhteet luovat vertailupohjan muille tarkasteluille. Perusasetukset voidaan valita seuraavista lähtökohdista:

1) Helpoin lähtökohta perusasetuksille on tasaisen todennäköisyysjakauman omaava informaation lähde. Mikäli jokaisella emissioympäristön symbolilla on sama todennäköisyys esiintyä, on entropia suurin mahdollinen ja täysin yksikäsitteisesti määritetty (ks. luku 3.2.2). Tällaisesta emissioympäristöstä käytetään merkintää E_U ja sen entropiasta merkintää H_{sU}.
2) Toinen lähtökohta perusasetuksille voisi olla emissiomalli, joka vastaisi esimerkiksi tyypillistä taistelutilannetta, jossa toiminnallisia tai taktisia rajoituksia lähettimien käytölle ei ole ja kaikki osajoukon lähettimet ovat aktiivisia tilanteelle tyypillisen todennäköisyysjakauman mukaisesti. Tällaiselle emissioympäristölle käytetään merkintää

E_E ja entropialle merkintää H_{sE}. Tämän tyyppisen perustilanteen etuna on muiden olosuhteiden vertailumahdollisuus suoraan johonkin käytännölliseen tilanteeseen. Suurimpana ongelmana lienee näiden käytännöllisten perusasetusten todennäköisesti melko työläs määrittäminen. Perusparametrien valinta saattaa vaatia huomatavan määrän analysointia ja evaluointi.

Tasaisesti jakautuneen emissioympäristön entropia on (vrt. luku 3.2.2):

$$H_{sU} = \log_2 n, \tag{4.18}$$

missä n = symbolien lukumäärä emissioympäristössä.

Muunlaisten diskreettien jakaumien osalta emissioympäristön entropia määritetään luvussa 3.2.4 esitettyjen yhtälöiden 3.6 ja 3.7 mukaisesti, eli:

$$H_s = \sum_i p_i \log_2 \frac{1}{p_i}, \text{ tai} \tag{4.19}$$

$$H_s = \sum_{i,j} \mu_i P_{ij} \log_2 \frac{1}{P_{ij}}. \tag{4.20}$$

Yllä olevissa määrittelyissä yksikkönä on bittiä/symboli, koska logaritmin kantalukuna on numero kaksi. Näin ollen tuotettu entropia ei ole sidottu aikaan, vaan jokaiseen tuotettuun symboliin. Entropia per symboli määrittelyn etuna on se, että siinä tarvitaan vähiten parametreja kuvaamaan emissioympäristön luonnetta ja tästä huolimatta erilaisten olosuhteiden vertailu keskenään on täysin mahdollista ja tuloksekasta.

Esimerkki 4.5

Tässä esimerkissä on laskettu entropia muutamille erilaisille emissiomalleille. Tuloksia tullaan hyödyntämään edempänä esitetyissä esimerkeissä. Tarkemmat laskutoimitukset on kirjattu liitteeseen 3.

Oletetaan, että osajoukot A, D ja F ja niitä mallintavat emissiomallit muodostuvat seuraavasti:

- Osajoukko A sisältää symbolit $A = \{a_1, a_2, a_3, a_4, a_5\}$, joita vastaa todennäköisyysjakauma $P(A = a_i) = p(a_i) = (0.143, 0.143, 0.143, 0.143, 0.428)$. Emissiomalli on kuvassa 4.7 esitetynlainen.

– Osajoukko D sisältää symbolit $D = \{d_1, d_2, d_3, d_4\}$. Emissiomalli on kuvan 4.8 mukainen. Siirtymätodennäköisyydet P_{ij} oletetaan alla olevan matriisin mukaisiksi.

$$P = \begin{pmatrix} 0.3 & 0.5 & 0.2 & 0 \\ 0.2 & 0.6 & 0.2 & 0 \\ 0.5 & 0 & 0 & 0.5 \\ 0.2 & 0 & 0.2 & 0.6 \end{pmatrix}$$

– Osajoukko F muodostuu kuvan 4.9 mukaisesta radiolinkkiverkosta. Yhtä linkkijännettä mallinnetaan kuvan 4.10 b mukaisella Markov ketjulla. Malli sisältää symboli $F = \{f_1, f_2\}$. Siirtymätodennäköisyydet P_{ij} ovat alla olevan matriisin mukaisesti:

$$P = \begin{pmatrix} P_{11} & P_{12} \\ P_{21} & P_{22} \end{pmatrix} = \begin{pmatrix} 0.1 & 0.9 \\ 0.9 & 0.1 \end{pmatrix}.$$

Taulukkoon 4.6 on laskettu kunkin osajoukon emissiomallia vastaava entropia sekä vertailukohdaksi ko. emissioympäristön suurin mahdollinen entropian arvo.

	Entropia [bit/symb]	Max entropia [bit/symb]
Osajoukko A	2.13	2.32
Osajoukko D	1.35	2
Osajoukko F - yksi linkkijänne	0.47	1
Osajoukko F - koko verkko	1.88	4

Taulukko 4.6: Yhteenveto osajoukkojen entropioista.

Eniten informaatiota tuottaa tulosten valossa osajoukko A. Sen tuottama entropia on myös varsin lähellä tasajakauman entropiaa. ◇

Mikäli halutaan määrittää emissioympäristön tuottaman entropian määrä aikayksikössä, voidaan hyödyntää luvussa 3.2.4 esitettyä yhtälöä 3.9. Jos emissiomalli on määritelty siten, että peräkkäisten symboleiden tuottaminen on toisistaan riippumaton toimenpide, voidaan tämän osajoukon tuottaman entropian nopeus laskea:

$$H_s' = \varphi \sum_i p_i \log_2 \frac{1}{p_i}, \qquad (4.21)$$

missä φ = prosessin symbolinopeus [symbolia/sek].

Jos osajoukon emissiomalli sisältää useita tiloja, määritetään osajoukon tuottaman informaation nopeus yhtälöllä (vrt. luku 3.2.4, yhtälöt 3.6 ja 3.9):

$$H_s^{'} = \sum_{ij} \varphi_i \mu_i P_{ij} \log_2 \frac{1}{P_{ij}} = \varphi_{avg} \sum_{ij} \mu_i P_{ij} \log_2 \frac{1}{P_{ij}}, \qquad (4.22)$$

missä φ_i = tilaa *i* vastaava symbolinopeus

φ_{avg} = tilojen symbolinopeuksien keskiarvo.

Lopputuloksena saadaan osajoukkojen keskimäärin tuottaman entropian määrä aikayksikössä (bittiä/sekunti). Osajoukon tuottaman entropian kokonaismäärä voidaan laskea, kun tiedetään miten pitkään osajoukon prosessi on toiminnassa. Merkitään tätä aikaa kirjaimella T_H. Kokonaisentropia, joka tuotettiin tämän ajan kuluessa on:

$$H_T = T_H H_s^{'}. \qquad (4.23)$$

Esimerkki 4.6

Esimerkin laskutoimitukset on esitelty liitteessä 3.

Oletetaan, että osajoukkojen A, D ja F emissiomallit ovat esimerkin 4.5 mukaiset. Lisäksi niihin liittyvät seuraavat symbolinopeudet:

- Osajoukkoa A kuvaavan emissiomallin symbolinopeus on φ = 0.5 symbolia/sekunti (malli tuottaa symbolin aina kahden sekunnin välein).
- Osajoukon D kutakin tilaa vastaavat seuraavat symbolinopeudet:

$$\varphi = \begin{pmatrix} \varphi_1 \\ \varphi_2 \\ \varphi_3 \\ \varphi_4 \end{pmatrix} = \begin{pmatrix} 0.2 \\ 0.1 \\ 0.05 \\ 0.2 \end{pmatrix}.$$

- Osajoukon F emissiomallin kumpaakin tilaa vastaa symbolinopeus $\varphi_1 = \varphi_2$ = 1000 symbolia/sek.

Taulukkoon 4.7 on laskettu kutakin emissiomallia vastaava entropian nopeus.

	Entropia [bit/sek]
Osajoukko A	1.06
Osajoukko D	0.19
Osajoukko F - yksi linkkijänne	470
Osajoukko F - koko verkko	1880

Taulukko 4.7: Esimerkin 4.6 tulokset.

Taulukosta 4.7 nähdään, että linkkijänteitä kuvaavien emissiomallien entropian nopeus on huomattavan suuri verrattuna muihin malleihin. Tämä johtuu suuresta symbolinopeudesta ja saattaa ylikorostaa linkkijänteiden tuottaman informaation merkitystä. Käytännössä vertailtaessa eri tyyppisiä osajoukkoja keskenään on parasta pitäytyä yksiköissä, joissa entropia ilmoitetaan symbolikohtaisesti (ks. esim. 4.5). ◇

Tiedustelujärjestelmän näkökulmasta katsottuna emissiomallin entropia näyttäytyy epävarmuutena tilanteesta, joka lähtökohtaisesti vallitsee emissioympäristössä. Informaatioteoreettisesta näkökulmasta katsoen on kuitenkin myös niin, että epävarmuus jonkin kokeilun lopputuloksesta ennen kokeen suorittamista on sama, kuin informaation määrän, joka odotetaan saatavan käyttöön kokeen toteuttamisen jälkeen [1, s. 29]. Jos oletetaan, että mitkään häiriötekijät eivät rajoita tiedustelujärjestelmän suorituskykyä, niin tällöin tiedustelujärjestelmä kykenee vastaanottamaan ja hyödyntämään kaiken informaation, mitä emissiomalli on kanavalle tuottanut. Tällaisessa tilanteessa voidaan mieltää, että tiedustelujärjestelmän kapasiteetin (merk. D) täytyy olla sama, kuin kanavan kapasiteetin, eli $C = D$. Luvun 3.2.5 mukaisesti tiedämme myös, että häiriöttömässä tilanteessa pätee $C \geq H_s$ ja käytännössä nyt voidaan lausua kaikille mahdollisille olosuhteille:

$$D \geq H_s . \tag{4.24}$$

Yllä oleva epäyhtälö korostaa, että häiriötön ympäristö soveltuu elektronisen aktiivisuuden ja elektronisen suojautumisen menetelmien arvioimiseen ainoastaan tilanteissa, joissa ei tarvitse kiinnittää huomiota vastustajan tiedustelukykyyn (koska se on aina vähintään yhtä suuri kuin tuotetun informaation määrä). Ainoa asia mitä häiriöttömässä tilanteessa voidaan arvioida, on emissiomallin lähtökohtaisesti tiedustelijalle tuottama epävarmuus. Tätä voidaan säädellä muuttamalla esiintymistodennäköisyysjakaumia tai vertailemalla eri määrän symboleita sisältäviä malleja. Jotta tarkasteluista saataisiin monipuolisempia, on olosuhteisiin lisättävä häiriöiden vaikutus.

4.3.3. Kuvautumistodennäköisyydet

Kuvautumistodennäköisyydet mallintavat, miten erilaiset häiriöt vaikuttavat emissiomallin sähkömagneettiseen spektriin tuottamiin symboleihin. Kuvautumistodennäköisyys määrittelee, millä todennäköisyydellä symboli lähtöjoukosta X kuvautuu kanavan yli juuri tietyksi symbo-

liksi tulojoukossa Y (vrt. luku 4.1.2). Kuvautumistodennäköisyys on ehdollinen todennäköisyys $P(Y|X = x) = c_{ij}$. Jatkotarkasteluissa kuvautumistodennäköisyyksillä tulee olemaan oleellinen merkitys määriteltäessä tiedustelujärjestelmän kapasiteettia ja edelleen arvioitaessa osajoukon elektronisen suojautumisen tasoa. Seuraavassa tarkastellaan, mitkä tekijät vaikuttavat kuvautumistodennäköisyyksiin.

Käytännössä kuvautumistodennäköisyys kertoo sen, millä todennäköisyydellä c_{ij} emissioympäristön ajan hetkellä t tuottama symboli x_i kuvautuu tiedustelujärjestelmän vastaanottamaksi symboliksi y_j. Kuvautumistodennäköisyyteen vaikuttavat seuraavat seikat:

- sieppaustodennäköisyys P_{POI}
- ilmaisutodennäköisyys P_D
- hyödyntämistodennäköisyys P_{EX}.

Symbolin (lähetteen, signaalin) sieppaamisella tarkoitetaan tilannetta, jossa tiedustelujärjestelmällä on valmiudet vastaanottaa symboli x_i juuri sillä hetkellä, kun emissioympäristö tuottaa ko. symbolin. Jotta symboli on siepattavissa, täytyy seuraavien olosuhteiden olla voimassa symbolin esiintymishetkellä: 1) Tiedusteluvastaanottimen tulee olla virittyneenä taajuusalueelle, jolla symboli esiintyy; 2) Mikäli tiedustelusensori käyttää keilaavaa suunta-antennia, tulee antennin pääkeilan osoittaa kohti lähetintä; 3) Jos lähettävässä laitteessa käytetään keilaavaa suunta-antennia, tulee antennin pääkeilan osoittaa kohti tiedustelusensoria (olettaen, että sieppaaminen sivukeiloista ei ole mahdollista) [71, s. 41]. Kaksi viimeistä ehtoa koskevat erityisesti elektronista mittaustiedustelua, jonka kohteina ovat tyypillisesti tutkat. Yleistäen voidaan sanoa, että mikäli tiedustelujärjestelmältä vaaditaan suurta sieppaustodennäköisyyttä ja laajaa valvontatilavuutta, tulee tällöin käyttää antennijärjestelmiä, jotka mahdollistavat jatkuvan 360 asteen valvontapeiton. Tällaiset ovatkin varsin käytettyjä taktisen tasan elektronisen tuen järjestelmissä [48, s. 295, 327 ja 348]. Suurin osa emissioympäristön lähettimistä käyttää ympärisäteileviä antenneja tai suunta-antenneja, jotka ovat kiinteästi suunnattu määrättyyn suuntaan [22, s. 30 - 40, 59, 107 - 119]. Näin ollen sieppaustodennäköisyyden määrittelee varsin usein tiedusteluvastaanottimen hetkellinen kaistanleveys ja aikamääreet, jotka ilmaisevat kuinka usein tiedusteluvastaanotin viritetään kullekin tiedusteltavalle taajuudelle ja miten pitkään dataa kultakin taajuudelta kerätään. Nykyaikaisissa elektronisen tuen järjestelmissä näitä parametreja voidaan yleensä säädellä jonkinlaisten hakuohjelmien avulla [15], [71] ja [72]. Tuntemalla tiedustelujärjestelmän ja emissioympäristön ominaisuudet, voidaan laskea, millä todennäköisyydellä erilaiset lähetteet kyetään sieppaamaan jonkin määrätyn ajan kuluessa. Siep-

paustodennäköisyyksien määrittämiseen ei tässä työssä perehdytä syvällisesti. Aihetta on käsitelty kirjallisuudessa esimerkiksi [13], [14], [15], [33], [53], [68], [70] ja [72].

Tässä työssä käsiteltävään mallinnukseen liittyen mielenkiinnon kohteena on se, kuinka iso osuus kutakin emissioympäristön tuottamaa symbolia voidaan sieppaustodennäköisyyden perusteella katsoa kuvautuvan oikein. Tuntemalla tilanteeseen vaikuttavat parametrit, tämä osuus on tapauskohtaisesti laskettavissa. Yksinkertaisempi lähestymistapa on tehdä seuraavat oletukset: 1) Tiedustelujärjestelmä kykenee suuntamaan tiedusteluvastaanottimien resurssia (kalustoa ja aikaa) enemmän niiden symboleiden sieppaamiseen, jotka ovat itsessään mielenkiintoisia ja/tai liittyvät johonkin kriittiseen toimintaan; 2) Pystymme päättelemään, mitkä ovat nämä joukon tai osajoukon kannalta kriittiset symbolit ja toiminnot. Näiden oletusten pohjalta voidaan luoda muutama kategoria määrittämään, millainen osuus kunkin kategorian symboleista on siepattavissa. Toisin sanoen kerrotaan, millainen osuus symboleista kuvautuu oikein sieppaustodennäköisyyden suhteen. Tarvittaessa voidaan rajoittaa niiden symboleiden määrää, joita eri luokkiin on mahdollista asettaa. Mallinnukseen liittyen prioriteettilistoille voidaan asettaa myös ajallisia rajoituksia siten, että jotkin symbolit ovat esimerkiksi korkeassa prioriteettiluokassa tietyn aikaikkunan ja alemmassa luokassa seuraavan. Tällä voidaan kuvata tiedusteluresurssin suuntaamista ajallisesti eri toimintoja vastaan. Kategoriat ja osuudet voitaisiin laatia esimerkiksi taulukon 4.8 mukaisesti.

Prioriteettiluokka	Symbolien määrä luokassa	Siepattavien osuus (P_{POI})
Prioriteetti 1	max 10 %	100 %
Prioriteetti 2	max 15 %	90 %
Prioriteetti 3	max 35 %	75 %
Prioriteetti 4	max 50 %	50 %
Prioriteetti 5	max 50 %	25 %

Taulukko 4.8: Esimerkki sieppaustodennäköisyyskategorioiden asettamisesta. Esitetyt luvut eivät perustu mihinkään analyysiin vaan ovat puhdas esimerkki.

Symbolin (lähetteen, signaalin) ilmaisussa on kyse siitä, saavuttaako siepattu symboli riittävän signaali/kohina-suhteen (*S/N*-suhde) tiedusteluvastaanottimella. *S/N*-suhteessa yhdistyvät kaikki tekijät, jotka vahvistavat hyötysignaalia sekä tekijät, jotka vahvistavat kohinaa. *S/N*-suhteelle määritetään raja-arvo (X dB), jonka yläpuolelle signaalin on päästävä, ennekuin se tulkitaan ilmaistuksi. Tyypillisesti tilanteeseen liittyy myös virheilmaisun mahdollisuus, joka huomioidaan ilmaisutodennäköisyyttä laskettaessa. Ilmaisutodennäköisyyden määrittämistä on tarkemmin käsitelty kirjallisuudessa mm. [25], [33], [53], [67], [68] ja [70].

Kyky ilmaista kulminoituu oikeastaan yhteen kysymykseen: Miltä etäisyydeltä ja miltä alueilta emissioympäristön tuottamat symbolit ovat tiedustelujärjestelmän ilmaistavissa? Tähän kysymykseen haetaan yleensä vastausta erilaisilla sähkömagneettisen säteilyn etenemistä kuvaavilla laskentamalleilla ja näitä malleja hyödyntävillä ohjelmistoilla [30, s. 101]. Yksinkertaisimmillaan etenemismalli voi perustua vapaantilan vaimennukseen tai vaikkapa radiohorisontin laskemiseen. Kehittyneempiä malleja, jotka huomioivat mm. erilaisten taajuusalueiden ja maastotyyppien ominaispiirteitä, on paljon ja niitä on esitelty kirjallisuudessa mm. [28], [33], [49] ja [59].

Elektronisen aktiivisuuden, elektronisen suojautumisen tason ja tiedustelujärjestelmän kapasiteetin arviointiin symbolin ilmaisu liittyy oleellisesti. Näin ollen myös tässä työssä esitellyt menetelmät vaativat rinnalleen laskentamenetelmän tai ohjelmiston, jonka avulla kyetään arvioimaan kunkin symbolin ilmaistavuus aikaan ja paikkaan sidottuna. Mallinnuksessa tulee huomioida myös käytetty kalusto mm. lähetystehojen, antennivahvistusten, kohinalukujen ja herkkyyksien osalta.

Oletetaan, että mallinnuksessa tarkastellaan aikaikkunaa, jonka pituus on T_E. Oletetaan lisäksi, että emissioympäristö sisältää symbolit $X = \{x_1, x_2, ..., x_n\}$, joita emissiomalli tuottaa esiintymistodennäköisyysjakauman $P(X)$ mukaisesti sekä keskimääräisellä symbolinopeudella φ_{avg}. Näiden tietojen perusteella voimme laskea, kuinka monta kappaletta kutakin symbolia on tuotettu tarkastelujakson aikana:

$$N_i = p(x_i)\varphi_{avg}T_E, \qquad i = 1, 2, \ldots, n. \tag{4.25}$$

Oletetaan vielä, että ympäristö on dynaaminen eli ainakin osa symboleista liikkuu tarkastelujakson aikana. Käyttämällä jotain etenemismallia, jokaiselle symbolille voidaan laskea aika T_i, jonka se on tiedustelujärjestelmän ilmaistavissa. Jos tiedustelujärjestelmä sisältää useita tiedustelusensoreita, voidaan laskea aikaikkunat, jolloin kukin symboli on ilmaistavissa erikseen jokaiselle sensorille. Symboli on tiedustelujärjestelmän ilmaistavissa aina, kun yksikin sensori sen kykenee ilmaisemaan. Edelleen voidaan laskea, kuinka monesti symboli x_i oli ilmaistavissa ajan T_i kuluessa:

$$N_{Di} = p(x_i)\varphi_{avg}T_i, \qquad i = 1, 2, \ldots, n. \tag{4.26}$$

Jokaista symbolia vastaava ilmaisusuhde P_{DRi} saadaan nyt laskettua

$$P_{DRi} = \frac{N_{Di}}{N_i} = \frac{T_i}{T_E} \leq 1, \qquad i = 1, 2, \ldots, n. \tag{4.27}$$

Ilmaisusuhde ei ole sama asia kuin ilmaisutodennäköisyys. Ilmaisusuhde riittää kuitenkin tässä esitetyissä tarkasteluissa kuvaamaan, millainen osuus symboleista on tarkastelujakson aikana ilmaistavissa. Kuten yllä esitetystä nähdään, ilmaisusuhde voidaan laskea myös suoraan aikojen T_i ja T_E suhteena.

Symbolin sieppaaminen ja ilmaisu muodostavat yhdessä symbolin havaitsemisen käsitteen [33, s. 277 ja 498], jonka voidaan katsoa tarkoittavan sitä, että emissioympäristön tuottaman symbolin olemassaolo on kyetty tiedustelujärjestelmässä todentamaan. Symbolin sieppaaminen ja ilmaisu eivät ole täysin toisistaan riippumattomia, koska niissä molemmissa on suuri merkitys käytetyllä kaistanleveydellä. Saattaa kuitenkin olla varsin vaikeaa määritellä yksiselitteisesti määriteltyä ehdollista todennäköisyyttä sieppaamisen ja ilmaisun kesken, koska molempiin tilanteisiin vaikuttaa myös monia muita tekijöitä, jotka ovat riippumattomia toisistaan. Näin ollen jokaista lähtöjoukon symbolia x_i vastaava havaitsemisen todennäköisyys määritellään yksinkertaisesti (vrt. esim. [33, s. 498])

$$P_{Hi} = P_{POIi} P_{DR\,i}, \qquad i = 1, 2, \ldots, n. \tag{4.28}$$

Mikäli mahdollisuuksia havaitun symbolin hyödyntämiseksi ei tarkasteluissa huomioida, voidaan kuvautumistodennäköisyydet lausua seuraavasti:

$$c_{ij} = \begin{cases} P_{Hi} & , \text{kun } i = j \\ 1 - P_{Hi} & , \text{kun } j = n+1 \\ 0 & , \text{muulloin} \end{cases}. \tag{4.29}$$

Toisin sanoen lähtöjoukon symboli x_i kuvautuu oikeaksi tulojoukon symboliksi y_j (missä $i = j$) havaitsemistodennäköisyydellä P_{Hi}. Symboli menetetään (tiedustelujärjestelmä ei kykene sieppaamaan ja/tai ilmaisemaan) todennäköisyydellä $1 - P_{Hi}$. Menetettyä symbolia kuvataan tulojoukossa symbolilla, jolla on indeksi $n + 1$. Menetetty symboli voidaan mieltää kuvautuneen ”välilyönniksi”.

On huomattava, että emissiomalli tuottaa jatkuvasti symboleita määrittelyidensä mukaisesti. Näin tapahtuu myös silloin, kun lähetin on tiedustelujärjestelmän kantaman ulkopuolella. Yllä olevan määrittelyn mukaisesti symboli kuvautuu tällöin ”välilyönniksi”. Jos lähetin on esimerkiksi radiohiljaisuudessa, sitä ei saa poistaa emissiomallista, koska tällöin malliin jääneiden lähettimien suhteelliset esiintymistodennäköisyydet kasvavat (koska osuuksien summan tulee aina olla yksi) ja tämä vääristää emissiomallia. Sen sijaan radiohiljaisuudessa olevan lähettimen tulee ajatella tuottavan symboleita, joiden lähetysteho on 0 wattia. Tällöin symboli ei ole ilmaistavissa, vaikka lähetin olisi tiedustelujärjestelmän kantaman piirissä. Näin ollen $P_{Hi} = 0$ ja kaikki symbolit kuvautuvat ”välilyönneiksi”. Samanlaista menettelyä noudatetaan kaikissa tilanteissa, joissa jokin häiriötekijä estää symbolin havaitsemisen (esim. maastoeste tai suunta-antennin minimi tiedustelijan suuntaan yms.).

Kyvyllä hyödyntää havaittu lähete (symboli) voidaan ymmärtää esimerkiksi mahdollisuudet suuntia/paikantaa, luokitella, analysoida tai purkaa (salaus) ko. symboli [33, s. 498]. Signaalien hyödyntämisen kannalta tärkeiden ulkoisten parametrien mittaustarkkuus riippuu oleellisesti saavutetusta *S/N*-suhteesta [70, s. 155 - 156]. Havaitseminen ei takaa hyödynnettävyyttä [33, s. 498], koska tyypillisesti riittävä parametrien mittaustarkkuus edellyttää suurempaa *S/N*-suhdetta, kuin signaalin ilmaisu. Tässä työssä symbolin hyödyntämisellä ymmärretään vain kyky yksiselitteiseen symbolin paikantamiseen. Jos kaksi tai useampi samaan symbolikategoriaan kuuluvaa symbolia sijaitsevat niin lähellä toisiaan, että niiden yksiselitteinen erottelu ei ole paikantamistarkkuuden puitteissa mahdollista, niin tällöin on vaarana, että symbolien kuvautumisessa tapahtuu virheitä. Suuntimisen, paikantamisen ja niiden tarkkuuden arviointiin kehitettyjä menetelmiä ja tekniikoita ei tässä työssä tarkasti käsitellä. Alue on varsin runsaasti tutkittu ja laajempaa käsittelyä sekä viitteitä tutkimuksiin löytyy kirjallisuudesta mm. [22], [48], [52], [53] ja [71].

Tyypillinen suuntimistarkkuus aina HF-alueelta ylöspäin on noin 1 – 2 astetta [3], [18], [21], [44], [45], [66] ja [69]. Näin ollen paikantamistarkkuus on tyypillisesti muutamia prosentteja tiedustelukannan ja lähettimen välisestä etäisyydestä [34, s. 36] ja [39, s. 171]. Esimerkiksi +/- 2° (rms) sunntimistarkkuudella voidaan saavuttaa 30 km etäisyydellä +/- 1 km:n paikantamistarkkuus [22, s. 120], joka on siis noin 3.3 % etäisyydestä.

Otetaan paikantamistarkkuuden lähtökohdaksi 5 % tiedustelujärjestelmän ja lähettimen välisestä etäisyydestä (merk. Δ). Jos ympyrän, jonka säde on $\delta = 0.05\Delta$, alueella on yksi tai useampi samaan symbolikategoriaan kuuluva lähetin, niin tällöin kuvautumistodennäköisyyksissä

on huomioitava, että symbolin kuvautuminen saattaa olla monikäsitteinen. Oletetaan, että lähettimet $X = \{x_1,...,x_m\}$, missä m voi olla m = 2, 3, …, n, kuuluvat samaan symbolikategoriaan ja sijaitsevat alle δ etäisyydellä lähettimestä $x_k \in X$. Tällöin hyödyntämistodennäköisyys P_{EXk} määritetään $P_{EXk} = 1/m$, eli yleisesti

$$P_{EXi} = \frac{1}{m_i}, \qquad i = 1, 2, \ldots, n. \qquad (4.30)$$

Tässä m_i = symbolin x_i kanssa samaan kategoriaan kuuluvien ja etäisyydellä < δ sijaitsevien symboleiden, ml. symboli x_i itse, lukumäärä.

Kun havaitsemisen ja hyödyntämisen todennäköisyydet yhdistetään, saadaan lähtöjoukon symbolia x_i vastaava käytettävyystodennäköisyys P_K, joka on

$$P_{Ki} = P_{Hi}P_{EXi} = P_{POIi}P_{DRi}P_{EXi}, \qquad i = 1, 2, \ldots, n. \qquad (4.31)$$

Kuvautumistodennäköisyydet voidaan nyt lausua seuraavasti:

$$c_{ij} = \begin{cases} P_{Ki} & \text{, kun } \exists \text{ mahdollisuus, että } x_i \mapsto y_j \text{ ja } j \neq n+1 \\ 1 - m_i P_{Ki} & \text{, kun } j = n+1 \\ 0 & \text{, muulloin} \end{cases}. \qquad (4.32)$$

Eli käytettävyystodennäköisyys määrää sellaisenaan kuvautumistodennäköisyyden aina, kun symboli kuvautuu oikein ($i = j$) ja myös silloin, kun symbolia ei kyetä yksiselitteisesti paikantamaan. Symboli menetetään todennäköisyydellä $1 - m_iP_{Ki}$. Luvussa 4.3.5 on esitelty tarkemmin hyödyntämisen todennäköisyyden huomioiminen tiedustelujärjestelmän kapasiteettia määriteltäessä.

4.3.4. Tiedustelujärjestelmän kapasiteetti ja häiriöiden huomioiminen

Absoluuttisella tiedustelujärjestelmän kapasiteetilla voidaan ymmärtää tiedustelujärjestelmään sisältyvien laitteiden (materiaalin), menetelmien ja henkilöstön muodostamaa suorituskykyä[12]. Absoluuttinen kapasiteetti voidaan mieltää maksimaaliseksi kyvyksi käsitellä dataa ja informaatiota sekä näiden jalostamista tietämykseksi (ks. tietoon liittyviä käsitteitä mm. [30, s.

[12] Vrt. suorituskyvyn määritelmä [32, s. 30 - 31]

60]). Absoluuttinen kapasiteetti (D_M) ei riipu ympäristön tuottamasta informaation määrästä (nopeudesta). Näin ollen voi olla $D_M \geq H_s'$ tai myös $D_M \leq H_s'$.

Suhteellisella tiedustelujärjestelmän kapasiteetilla (D_R) ilmaistaan, kuinka paljon ympäristön tuottamasta informaatiosta (H_s) tiedustelujärjestelmä kykenee vastaanottamaan. Suhteellinen kapasiteetti määritellään siten, että $D_R \leq H_s \leq H_{sU}$. Näin ollen on aina:

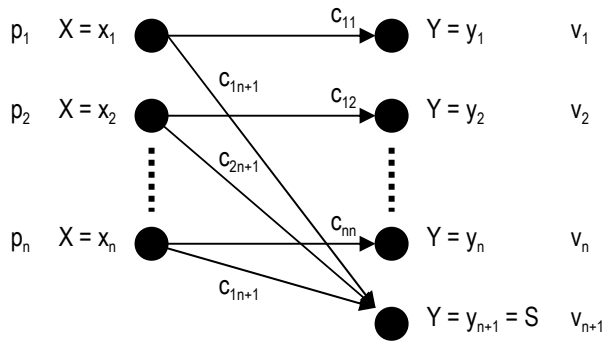
$$\frac{D_R}{H_{sU}} \leq \frac{D_R}{H_s} \leq 1. \qquad (4.33)$$

Edellä on kerrottu (ks. luku 4.3.2), että H_{sU} edustaa tasajakaumaa noudattelevan emissioympäristön (E_U) entropiaa ja tällöin entropia on suurin mahdollinen. Tämä muodostaa ehdottoman maksimin tiedustelujärjestelmän suhteelliselle kapasiteetille. Suhteellinen kapasiteetti ei myöskään koskaan voi ylittää emissioympäristön tuottaman informaation määrää, koska tämä on arvo, jonka suhteen kapasiteetti tullaan laskemaan. On huomattava, että tiedustelujärjestelmän suhteellista kapasiteettia ei voi vaatia olemaan aina pienempi tai yhtä suuri kuin tyypillistä emissioympäristöä E_E vastaava entropia H_{sE}. Nimittäin, jos emissiomallin esiintymistodennäköisyydet asetetaan siten, että $H_{sE} < H_s$, niin tällöin voi hyvinkin päteä $H_{sE} < D_R \leq H_s$. Entropiaa H_{sE} voidaan toki käyttää kiinnitettynä vertailupisteenä, johon muita tehtyjä tarkasteluita verrataan.

Suhteellista kapasiteettia määriteltäessä huomioidaan ilmiöt, jotka vaikeuttavat tiedustelujärjestelmän toimintaa. Nämä ilmiöt kulminoituvat kolmeen tekijään; symbolien sieppaaminen, symbolien ilmaisu ja symbolien hyödyntäminen. Hyödyntämistodennäköisyyttä ei tämän luvun tarkasteluissa huomioida. Tätä tekijää on käsitelty tarkemmin luvussa 4.3.5. Häiriöttömässä tilanteessa kaikki symbolit ovat siepattavissa, ilmaistavissa ja hyödynnettävissä ja tällöin $D_R = H_s$ (vrt. luku 4.3.2). Tämä tilanne on mahdollista saavuttaa myös häiriöllisessä ympäristössä, mikäli jokainen symboli on havaittavissa ja hyödynnettävissä 100 % todennäköisyydellä.

Voidaan olettaa, että jokaisen emissiomallin tuottaman symbolin kohdalla tiedustelujärjestelmän kyky siepata ja ilmaista tuo symboli tarkistetaan erikseen ja muista symboleita riippumattomasti. Jos tarkistus on positiivinen molempien kriteerin kohdalla, voidaan olettaa symboli oikein vastaanotetuksi. Jos yksikin kriteereistä on negatiivinen, oletetaan symboli hukatuksi. Tämä tarkistus ei ota huomioon mahdollisuutta, että onnistuneesti vastaanotettu symboli tul-

kittaisiin joksikin muuksi symboliksi. Tätä mahdollisuutta on käsitelty jäljempänä hyödyntämistodennäköisyyden kohdalla. Symbolien kuvautumista emissioympäristöstä tiedustelujärjestelmään voidaan havainnollistaa kuvan 4.11 mukaisesti. Lopputuloksena tällaisesta symbolien kuvautumisesta on symbolijono, joka vastaa onnistuneesti vastaanotettujen symbolien osalta emissiomallin tuottamaa jonoa, mutta hukattujen symbolien kohdalla on aukko (”välilyönti”). Muodostuneelle symbolijonolle voidaan laatia todennäköisyysmassafunktio, josta paljastuu kunkin symbolin suhteellinen esiintyminen ko. jonossa. Käsitteellä vastaanottotodennäköisyysjakauma $P(Y = y_j) = p(y_j) = v_j$ ymmärretään kaikkien vastaanotettujen symbolien (ml. ”välilyönnit”) jakaumaa. Tiedustelutodennäköisyysjakaumalla tarkoitetaan vastaanotettujen symbolien suhteellista keskinäistä jakaumaa, kun ei enää huomioida menetettyjä symboleita (”välilyöntejä”).



Kuva 4.11: Symboleiden lähtöjoukko muodostuu symboleista x_i, jotka esiintyvät emissioympäristössä todennäköisyydellä p_i. Symbolit kuvautuvat kanavan yli kuvautumistodennäköisyyksien c_{ij} mukaisesti, joko oikein tai sitten symboli menetetään (kuvautuu symboliksi y_{n+1}. Tulojoukko muodostuu symboleista y_j ja niiden jakaumaa kuvaavat vastaanottotodennäköisyydet v_j.

Suhteellinen tiedustelujärjestelmän kapasiteetti määritellään samantyyppisesti, kuin on alun perin määritelty informaation lähteen todellinen lähetysnopeus (R) (ks. luku 3.2.5). Voidaan siis lausua

$$D_R = H_s(X) - H(X \mid Y) = I(X;Y), \qquad (4.34)$$

missä $H_s(X)$ on emissioympäristön sähkömagneettiseen spektriin tuottama informaation määrä (entropia) ja ehdollinen entropia $H(X|Y)$ kuvaa kaikkia häiriöiden vaikutuksia, jotka vähentävät tiedustelujärjestelmän kykyä vastaanottaa emissioympäristön muodostamia symboleita. Emissioympäristöä mallinnetaan emissiomallin avulla (vrt. luvut 4.1.1 ja 4.3.1). Satunnaismuuttuja X kuvaa emissioympäristön tuottamia symboleita ja satunnaismuuttuja Y kuvaa tiedustelujärjestelmän vastaanottamia symboleita. Häiriöillä ymmärretään tässä yhteydessä kaik-

kia poikkeamia verrattuna optimitilanteeseen. Kaikki sisäiset ja ulkoiset kohinalähteet voidaan huomioida ilmaisutodennäköisyyttä määriteltäessä [68, s. 48 - 65]. Sieppaustodennäköisyyden poikkeamat optimaalisesta (100 % todennäköisyys) mielletään myös häiriöiksi, vaikka ne sinänsä polveutuvat luonnollisella tavalla käytetyn tekniikan ominaisuuksista.

Yllä esitetyn yhtälön 4.34 mukaisesti tiedustelujärjestelmän suhteellinen kapasiteetti on sama, kuin on satunnaismuuttujien *X* ja *Y* välinen yhtenäisinformaatio (ks. luku 3.2.8). Määritelmä on varsin luonnollinen, koska yhtenäisinformaatio ymmärretään *X*:n epävarmuuden vähentymiseksi, kun *Y* tunnetaan [16, s. 21]. Toisin sanoen, kuinka paljon tiedustelujärjestelmän tuottama tieto selventää käsitystä siitä, mitä todellisuudessa tapahtui. Tässä kohdin on syytä huomata, että tällä tavoin määriteltynä tiedustelujärjestelmän kapasiteetti ei huomioi millään tavalla kykyä arvioida tulevia tapahtumia, joka on tyypillisesti eräs tiedustelujärjestelmän tehtävä. Joukon elektronisen aktiivisuuden ja elektronisen suojautumisen arvioinnissa tällä rajoituksella ei ole suurta merkitystä.

Yllä mainittu ehdollinen entropia lasketaan [62, s. 12], [16, s. 17 - 18]

$$H(X \mid Y) = \sum_{x,y} p(x,y) \log_2 \frac{1}{p(x \mid y)}. \qquad (4.35)$$

Voidaan osoittaa (ks. liite 4), että miellettäessä kanava kuvan 4.11 mukaiseksi, eli lähetetty symboli x_i vastaanotetaan samantyyppisenä symbolina tai vaihtoehtoisesti sitä ei vastaanoteta ollenkaan (S = ”välilyönti”), niin tällöin ehdollinen entropia typistyy muotoon

$$H(X \mid Y) = \sum_{x} p(x, y = S) \log_2 \frac{1}{p(x \mid y = S)}. \qquad (4.36)$$

Ehdollisen entropian luonnetta ja merkitystä voidaan vielä selventää toteamalla, että se ei niinkään kuvaa sitä, kuinka paljon symboleita jäi vastaanottamatta, vaan se kuvaa sitä informaation määrää, joka lähetettiin ja jota ei saatu vastaanotettua. Ehdollisen entropian luonnetta voidaan havainnollistaa myös alla olevan esimerkin tuloksilla; voidaan todeta, että keskimäärin 81.3 % symboleista saadaan vastaanotettua, mutta informaatiosta saadaan vastaanotettua n. 87 %.

Erilaisten olosuhteiden vertailu on suoraan helpointa, kun normalisoidaan yhtälö 4.34. Näin aikaansaatavaa määrittelyä kutsutaan tiedustelujärjestelmän normalisoiduksi kapasiteetiksi ja se lausutaan

$$D_N = \frac{1}{H_s(X)}\big(H_s(X) - H(X \mid Y)\big) = 1 - \frac{H(X \mid Y)}{H_s(X)}, \qquad (4.37)$$

missä $0 \le D_N \le 1$, koska aina pätee $H(X \mid Y) \le H_s(X)$.

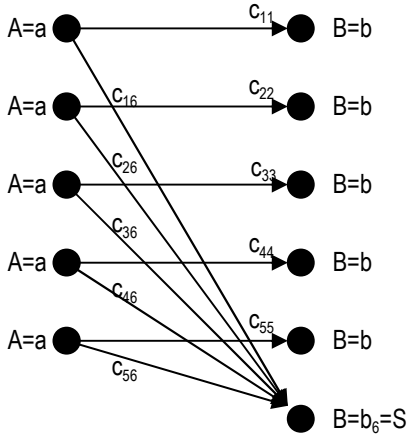
Yhtälö 4.37 saa arvon yksi, kun tarkasteltava tilanne on täysin häiriötön. Mitä enemmän häiriöt vaikeuttavat informaation kuvautumista, sitä pienemmäksi normalisoitu kapasiteetti käy.

Esimerkki 4.7

Esimerkin täydelliset laskutoimitukset ja välivaiheet on esitetty liitteessä 4.

Tarkastellaan jälleen tilannetta, jossa emissioympäristön muodostavat viisi symbolia $A = \{a_1, a_2, a_3, a_4, a_5\}$ ja joiden aktiivisuutta mallintaa kuvan 4.7 mukainen emissiomalli (ks. myös esimerkki 4.5). Oletetaan, että tiedustelujärjestelmän vastaanottaessa symboleita, symbolit $a_1 - a_4$ havaitaan todennäköisyydellä $P_{Hi} = 0.9$ (kun $i = 1 - 4$) ja symboli a_5 havaitaan todennäköisyydellä $P_{H5} = 0.7$. Yhtälön 4.29 perusteella muodostettu kuvautumistodennäköisyysmatriisi (kanavamatriisi) on esitetty alla. Symbolien kuvautumista voidaan havainnollistaa kuvan 4.12 mukaisesti.

$$C = \begin{pmatrix} c_{11} & c_{12} & c_{13} & c_{14} & c_{15} & c_{16} \\ c_{21} & c_{22} & c_{23} & c_{24} & c_{25} & c_{26} \\ c_{31} & c_{32} & c_{33} & c_{34} & c_{35} & c_{36} \\ c_{41} & c_{42} & c_{43} & c_{44} & c_{45} & c_{46} \\ c_{51} & c_{52} & c_{53} & c_{54} & c_{55} & c_{56} \end{pmatrix} = \begin{pmatrix} 0.9 & 0 & 0 & 0 & 0 & 0.1 \\ 0 & 0.9 & 0 & 0 & 0 & 0.1 \\ 0 & 0 & 0.9 & 0 & 0 & 0.1 \\ 0 & 0 & 0 & 0.9 & 0 & 0.1 \\ 0 & 0 & 0 & 0 & 0.7 & 0.3 \end{pmatrix}$$



Kuva 4.12: Symbolien kuvautuminen kanavan yli.

Yhtälön 4.34 perusteella saadaan tiedustelujärjestelmän suhteelliseksi kapasiteetiksi

$$D_R = I(A;B) = H_s(A) - H(A \mid B) = 2.1290 \frac{bit}{symboli} - 0.2798 \frac{bit}{symboli} \approx 1.85 \frac{bit}{symboli}.$$

Tiedustelujärjestelmän normalisoitu kapasiteetti on

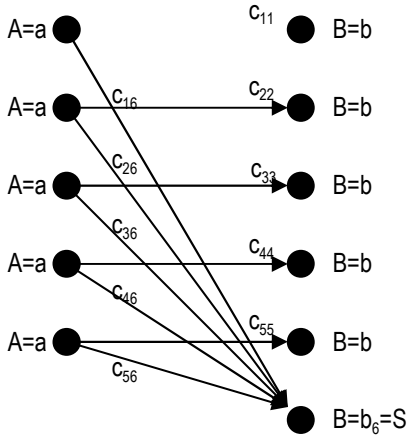
$$D_N = 1 - \frac{H(A \mid B)}{H_s(A)} = 1 - \frac{0.2798}{2.1290} \approx 0.869.$$

Näin ollen tiedustelujärjestelmä kykenee vastaanottamaan keskimäärin lähes 87 % emissioympäristön tuottamasta informaatiosta. Kaikista aktiivisista symboleista tiedustelujärjestelmä kykenee havaitsemaan noin 81 %. ◇

Esimerkki 4.8

Tarkastellaan seuraavaksi tilannetta, jossa lähetin a_1 on radiohiljaisuudessa ja tuottaa näin ollen symboleita, jotka kaikki kuvautuvat ”välilyönneiksi” (ks. luku 4.3.3). Kanavamatriisi on esitetty alla. Tällöin tilanne muodostuu kuvan 4.13 mukaiseksi.

$$C = \begin{pmatrix} c_{11} & c_{12} & c_{13} & c_{14} & c_{15} & c_{16} \\ c_{21} & c_{22} & c_{23} & c_{24} & c_{25} & c_{26} \\ c_{31} & c_{32} & c_{33} & c_{34} & c_{35} & c_{36} \\ c_{41} & c_{42} & c_{43} & c_{44} & c_{45} & c_{46} \\ c_{51} & c_{52} & c_{53} & c_{54} & c_{55} & c_{56} \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0.9 & 0 & 0 & 0 & 0.1 \\ 0 & 0 & 0.9 & 0 & 0 & 0.1 \\ 0 & 0 & 0 & 0.9 & 0 & 0.1 \\ 0 & 0 & 0 & 0 & 0.7 & 0.3 \end{pmatrix}$$



Kuva 4.13: Symbolien kuvautuminen kanavan yli.

Tiedustelujärjestelmän suhteelliseksi kapasiteetiksi saadaan

$$D_R = 2.1290 - 0.5195 = 1.6095 \frac{bit}{symboli}.$$

Normalisoitu kapasiteetti on: $D_N = 0.756$, eli noin 76 % informaatiosta.

Yllä olevista esimerkeistä havaitaan, että yhden lähettimen asettaminen radiohiljaisuuteen vähensi tiedustelujärjestelmän saataville päätyvän informaation määrää noin 11 %. Voidaan siis sanoa, että elektronisen aktiivisuuden taso on esimerkissä 4.8 11 % pienempi, kuin esimerkin 4.7 tilanteessa. On siis saatu tuotettua selkeä mitallinen tulos. ◇

Tiedustelujärjestelmän normalisoitu kapasiteetti antaa selkeitä vertailukelpoisia tuloksia. Oletetaan, että vertaillaan kahta emissiomallia, joiden entropiat ovat erisuuruiset. Lisäksi oletetaan, että emissiomallien tuottama informaatio kuvautuu häiriöllisen kanavan yli samansuuruisella normalisoidulla kapasiteetilla. Voidaanko nyt tulkita, että tiedustelujärjestelmällä on riittävä tieto rakentaa yhtä hyvä tilannekuva kummassakin tapauksessa. Tulkinta on oikein suhteessa emissiomallin vaikeusasteeseen nähden, koska normalisoitua kapasiteettia hyödynnettäessä tulokset ilmaistaan aina suhteessa emissiomallin tuottamaan entropiaan. Tämä on myös yleensä täysin riittävä tarkastelutapa, mikäli vertaillaan erilaisten elektronisten suojautumiskeinojen vaikutuksia tiedustelujärjestelmän ulottuville päätyvän informaation määrään.

Suhteellinen vertailutapa aiheuttaa kuitenkin myös erään rajoitteen esitetyn menetelmän käytölle. Tämä johtuu siitä, että absoluuttisesti tiedustelijan ulottumattomiin päätyvän informaation määrää voidaan mitata tiedustelujärjestelmän suhteellisen tai normalisoidun kapasiteetin avulla vain tilanteissa, joissa emissiomallin esiintymistodennäköisyydet pysyvät samoina (ja tällöin emissiomallin entropia on koko ajan sama). Toisin sanoen, mikäli halutaan absoluuttisesti vertailukelpoisia tuloksia eri olosuhteiden välille, voidaan mallinnuksessa säätää vain kuvautumistodennäköisyyksiä. Emissiomalliin liittyviä esiintymistodennäköisyyksiä tai symbolinopeuksia ei voida muuttaa. Jotta erilaisten olosuhteiden vertailtavuus säilyisi kaikissa tilanteissa, on tiedustelujärjestelmän suhteellisen ja normalisoidun kapasiteetin rinnalle nostettava vertailu, joka perustuu ehdolliseen entropiaan. Paneudutaan tähän analysoimalla tarkemmin yllä esitettyä kahden erilaisen entropian omaavan emissiomallin tilannetta.

Tarkastellaan kahta emissiomallia A_1 ja A_2, joiden erona on se, että mallille A_1 annettu esiintymistodennäköisyysjakauma tuottaa suuremman entropian, kuin mallin A_2 jakauma, eli $H_s^{A1} > H_s^{A2}$. Kiinnitetään tiedustelujärjestelmän normalisoitu kapasiteetti siten, että $D_N^{A1} = D_N^{A2} = k$, missä $k \in [0,1[$. Nyt voidaan osoittaa (ks. liite 5), että millä tahansa *k*:n arvolla ehdollisille entropioille pätee

$$H^{A1}(\cdot\,|\,\cdot) > H^{A2}(\cdot\,|\,\cdot)\,. \qquad (4.38)$$

Tulos voidaan tulkita siten, että vaikka suhteellisesti ottaen tiedustelijalle päätyvä informaation määrä on olosuhteiden kesken sama, niin tilanteessa A_1 tiedustelija menettää aina absoluuttisesti enemmän informaatiota. Ehdollinen entropia voidaan mieltää keskimääräiseksi lisäinformaatioksi, joka tulisi lähettää kanavalle symbolia kohden (tai aikayksikössä), jotta kaikki informaatio saataisiin siirrettyä oikein vastaanottajalle [62, s. 20 - 21]. Tiedustelujärjestelmän kannalta tämä voisi karkeasti tarkoittaa, että ehdollisen entropian verran informaatiota on kyettävä keräämään jollain muulla tavalla.

Tulos 4.38 johtaa suoraan myös päätelmään, että tiedustelujärjestelmä menettää aina absoluuttisesti eniten informaatiota silloin, kun esiintymistodennäköisyysjakauma on tasajakauma. Näin on, koska $H_{sU}(P_U) > H_s(P)$ (ks. luku 3.2.2). Tässä P_U on tasajakauma ja P mikä tahansa tasajakaumasta poikkeava jakauma. Samojen oletusten ollessa voimassa, kuin lauseketta 4.38 johdettaessa, täytyy nyt olla voimassa epäyhtälö

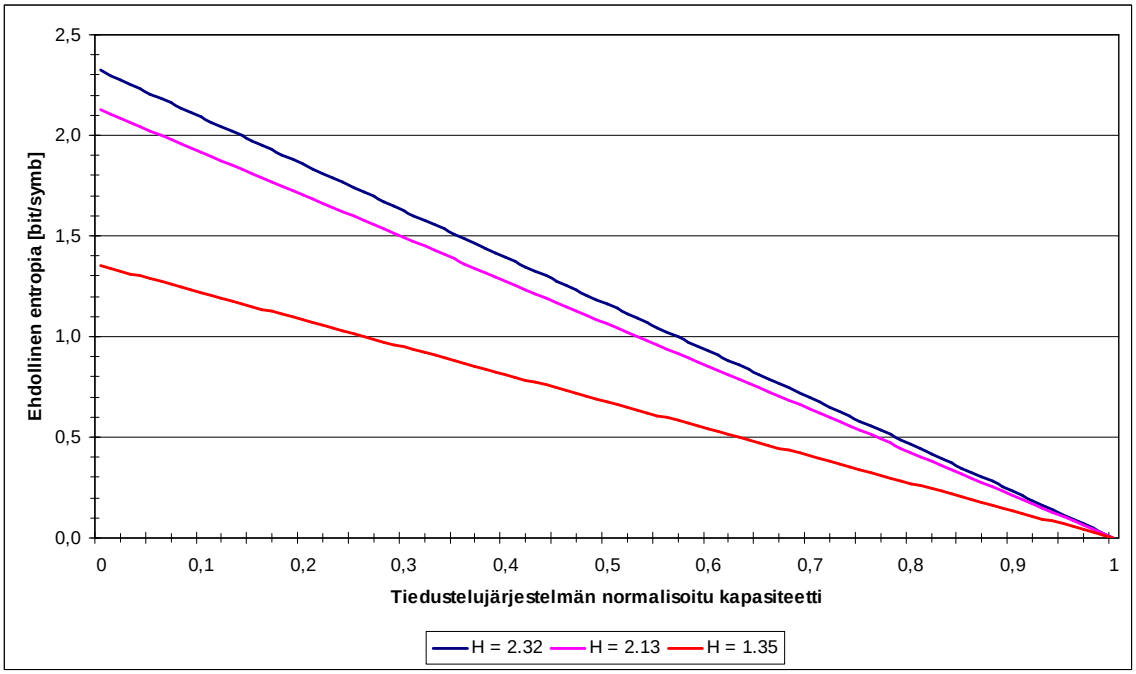
$$H_{sU}(\cdot\,|\,\cdot) > H_s(\cdot\,|\,\cdot)\,. \qquad (4.39)$$

4.39 todistaa osaltaan, että mahdollisimman tasaisesti eri lähetinyksilöiden välille jakautunut aktiivisuus on elektronisen suojautumisen kannalta paras vaihtoehto. Esimerkin muodossa tähän palataan luvussa 5.4.3.

Yhtälö 4.37 saadaan helposti muotoon

$$H(\cdot\,|\,\cdot) = -H_s D_N + H_s\,. \qquad (4.40)$$

Yhtälön 4.40 avulla saadaan määritettyä ehdollisen entropian arvo mille tahansa entropian ja normalisoidun kapasiteetin arvoille. Erilaisia tilanteita voidaan myös tarkastella esittämällä ehdollinen entropia tiedustelujärjestelmän normalisoidun kapasiteetin funktiona erilaisille emissiomallin entropian arvoille. Esimerkki tällaisista kuvaajista on kuvassa 4.14.



Kuva 4.14: Ehdollinen entropia esitettynä normalisoidun kapasiteetin funktiona. Ylin suora vastaa osajoukon A entropiaa, kun esiintymistodennäköisyydet ovat tasajakautuneet. Keskimmäinen suora saadaan käyttämällä osajoukon A alkuperäisiä määrittelyitä (ks. esimerkki 4.5). Alin kuvaaja vastaa osajoukon D emissiomallin entropiaa (ks. esimerkki 4.5).

Koska ehdollinen entropia on yhtälössä 4.40 ja kuvassa 4.14 määritetty normalisoidun kapasiteetin suhteen, voidaan nyt vertailla mitä tahansa olosuhteita keskenään. Käytännössä ei ole merkitystä ovatko vertailtava tulokset saatu muuttamalla saman emissiomallin (symbolien lukumäärä pysyy samana) todennäköisyysarvoja vai onko kyseessä kokonaan eri emissiomalli. Esimerkiksi kuvan 4.14 kuvaajien avulla voidaan aina vertailla kahden erilaisen normalisoidun kapasiteetin aikaan saamaa ehdollista entropiaa. Voidaan tulkita, että se olosuhde, joka tuottaa suuremman ehdollisen entropian, on lähtökohtaisesti paremmassa asemassa elektronista aktiivisuutta ja elektronisen suojautumisen tasoa arvioitaessa.

Esimerkki 4.9

Oletetaan, että osajoukon D entropian kuvautuessa kanavan yli, tiedustelujärjestelmän normalisoiduksi kapasiteetiksi saadaan $D_N^D = 0.55$. Osajoukon A tuottama entropia on suurempi kuin osajoukon D tuottama. Määritelmän 4.38 perusteella tiedetään, että tällöin A:n ehdollinen entropia on aina suurempi, jos normalisoidut kapasiteetit ovat samat. Mutta kuinka paljon suurempi osajoukon A normalisoitu kapasiteetti saa olla, ennekuin sen elektronisen aktiivisuuden tason voidaan katsoa olevan huonomman, kuin osajoukolla D?

Yhtälön 4.40 perusteella nähdään, että kapasiteettia $D_N^D = 0.55$ vastaa ehdollinen entropia $H^D(\cdot\,|\,\cdot) = 0.6091 \frac{bit}{symb}$. Asettamalla $H^A(\cdot\,|\,\cdot) = H^D(\cdot\,|\,\cdot)$ voidaan laskea raja-arvo, jota suu-

remmilla normalisoidun kapasiteetin arvoilla osajoukon A ehdollinen entropia on pienempi, kuin osajoukon D. Raja-arvoksi saadaan

$$D_N^A = 1 - \frac{H^A(\cdot\,|\,\cdot)}{H_s^A} = 1 - \frac{0.6091}{2.1290} \approx 0.714.$$

Laskettu tilanne on hahmotettavissa myös kuvasta 4.14.

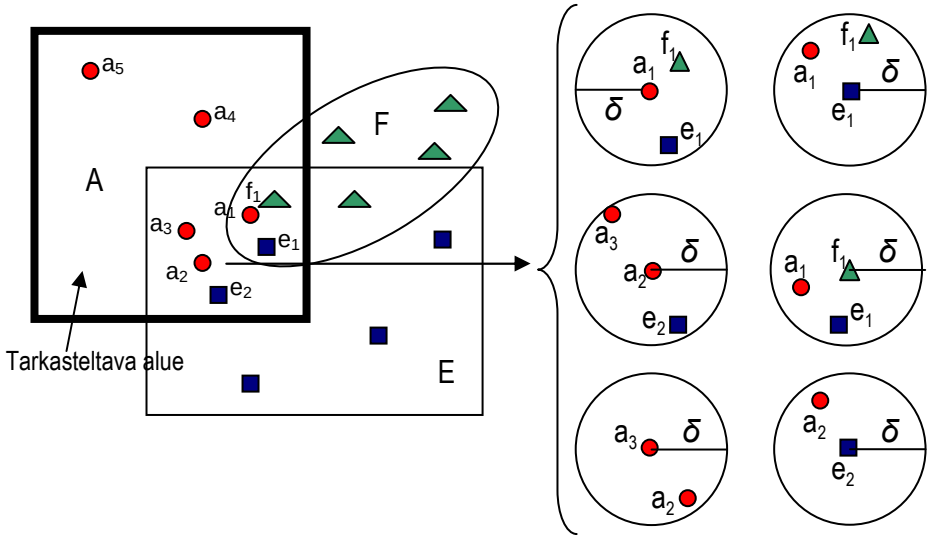
Voidaan siis tulkita, että osajoukon D tuottamasta informaatiosta jää absoluuttisesti enemmän tiedustelijan ulottumattomiin, jos $D_N^A > 0.714$. Osajoukon A kohdalla tiedustelujärjestelmän normalisoitu kapasiteetti saa olla noin 0.16 yksikköä suurempi kuin osajoukolla D, ennekuin sen elektronisen aktiivisuuden tason voidaan katsoa olevan huonomman. ◇

4.3.5. Hyödyntämistodennäköisyyden vaikutus tiedustelujärjestelmän kapasiteettiin

Mikäli mallinnuksessa huomioidaan vain mahdollisuudet symbolin sieppaamiseen ja ilmaisuun, niin tällöin tiedustelujärjestelmän kapasiteetin määrittäminen toteutetaan luvussa 4.3.4 esitettyjen periaatteiden mukaisesti. Tässä luvussa tuota tarkastelua täydennetään käsittelemään myös tilanteita, joissa symbolien paikantaminen ei ole yksiselitteistä ja tällöin on huomioitava hyödyntämistodennäköisyyden vaikutus tiedustelujärjestelmän kapasiteettiin. Tässä vaiheessa on myös huomioitava tilanteet, joissa erilliset osajoukot ovat limittyneet siten, että kahteen tai useampaan eri osajoukkoon sisältyviä ja samaa lähetekategoriaa edustavia symboleita sijaitsee lähekkäin. On huomattava, että mikäli muodostetut osajoukot noudattelevat eri taajuuksia käyttävien radioverkkojen rajoja, on tällöin symbolien erottelu mahdollista taajuuden perusteella, vaikka osajoukot olisivat limittyneinä toisiinsa. Tällainen erottelu ei kuitenkaan välttämättä ole mahdollista etenkin, jos symboleita tuottavat nykyaikaiset hyppivätaajuiset lähettimet ja/tai viestiverkko perustuu ad hoc – tyyppiseen rakenteeseen, jossa on mahdollista käyttää samaa taajuutta laajalla alueella ja lukumääräisesti suuressa määrässä lähettimiä [38, s. 130]. Seuraavassa tarkastelussa oletetaan, että symbolien erottelu käytettyjen taajuuksien perusteella ei ole mahdollista.

Luvussa 4.3.3 valittiin paikantamistarkkuuden kriteeriksi 5 % tiedustelukannan ja kohteen välisestä etäisyydestä (Δ). Näin ollen, jos samaan lähetekategoriaan kuuluvia symboleita on tarkastelun kohteena olevalla alueella lähempänä kuin δ toisistaan ($\delta < 0.05\Delta$), on tämä huomioi-

tava kuvautumistodennäköisyyksiä määritettäessä. Tarkasteltava tilanne muodostuu kuvan 4.15 kaltaiseksi.



Kuva 4.15: Kolme limittynyttä osajoukkoa A, E ja F. Mikäli jokin toinen samaan lähetekategoriaan kuuluva symboli sijaitsee $\delta < 0.05\Delta$ etäisyydellä toisesta symbolista, on paikannus monikäsitteinen ja tämä on huomioitava kuvautumistodennäköisyyksissä.

Tarkastelua varten on muodostettava uusi emissiomalli, jossa tarkasteltavan osajoukon muodostamassa informaatiossa on huomioitava limittyneiden osajoukkojen vaikutus. Kuvan 4.15 tapauksessa on siis rakennettava emissiomalli osajoukolle A siten, että osajoukkojen E ja F limittyvät symbolit lisätään uuteen malliin. Tämän jälkeen tarkastelu noudattelee varsin pitkälti luvussa 4.3.4 esiteltyjä menetelmiä.

Oletetaan, että osajoukkojen emissiomallit tuottavat symboleita aikavälin $[t_1, t_2] = \Delta t$. Tuona aikana kunkin osajoukon tuottamien symboleiden lukumäärä on $N_k = \varphi_k \cdot \Delta t$, missä φ_k on osajoukolle tyypillinen symbolinopeus. Erillisten osajoukkojen emissiomallien esiintymistodennäköisyysjakaumien perusteella voidaan arvioida kuinka monta kutakin symbolia tuotettiin. Tämä lasketaan

$$N_{k(z)} = \mu_{k(z)} N_k = \mu_{k(z)} \varphi_k \Delta t \,, \qquad (4.41)$$

missä $k(z)$ = osajoukon tunnus (k) ja symbolin tunnus (z)
(huom. kuvan 4.15 esimerkissä k on A, E tai F)
$\mu_{k(z)}$ = Markov ketjun rajatodennäköisyys. Jos peräkkäiset symbolit ovat riippumattomia, niin $\mu_{k(z)} = p_{k(z)}$.

Tarkasteltavan osajoukon alueella (merk. A) yhteensä tuotettujen symbolien lukumäärä saadaan laskemalla yhteen niiden symbolien lukumäärät, jotka sijaitsevat ko. alueella. Lausutaan tämä seuraavasti

$$N_A = \sum_{z \in A} N_{k(z)} = \sum_{i=1}^{h} N_i \,, \qquad (4.42)$$

missä h = tarkasteltavalla alueella sijaitsevien symboleiden lukumäärä.

Yksinkertaisimmassa tapauksessa uusi emissiomalli voidaan muodostaa olettamalla peräkkäisten symbolien valinnan olevan riippumattomia toisistaan. Tällöin jokaista tarkasteltavalla alueella sijaitsevaa symbolia α_i vastaava tilastollinen esiintymistodennäköisyys saadaan

$$\pi(\alpha_i) = \frac{N_i}{N_A}, \qquad i = 1, 2, \ldots, h. \qquad (4.43)$$

Lopputuloksena on siis tarkasteltavalla alueella A sijaitseva symbolijoukko (lähtöjoukko) $\alpha = \{\alpha_1, \alpha_2, ..., \alpha_h\}$ ja symboleiden esiintymistä kuvaava täydellinen todennäköisyysjakauma $\pi(\alpha = \alpha_i) = \pi(\alpha_i)$, missä $i = 1, ..., h$. Korvaamalla alkuperäistä osajoukkoa merkinnyt kirjain A tuolla alueella sijaitsevien symbolien joukkoa kuvaavalla kirjaimella α, saadaan yhtälö 4.43 muotoon

$$\pi(\alpha_i) = \frac{N_i}{N_\alpha} = \frac{N_{k(z)}}{\sum_{z \in \alpha} N_{k(z)}} = \frac{\mu_{k(z)} \varphi_k \Delta t}{\Delta t \sum_{z \in \alpha} \mu_{k(z)} \varphi_k} = \frac{\mu_{k(z)} \varphi_k}{\sum_{z \in \alpha} \mu_{k(z)} \varphi_k}, \qquad (4.44)$$

missä $i = 1, \ldots, h$ ja

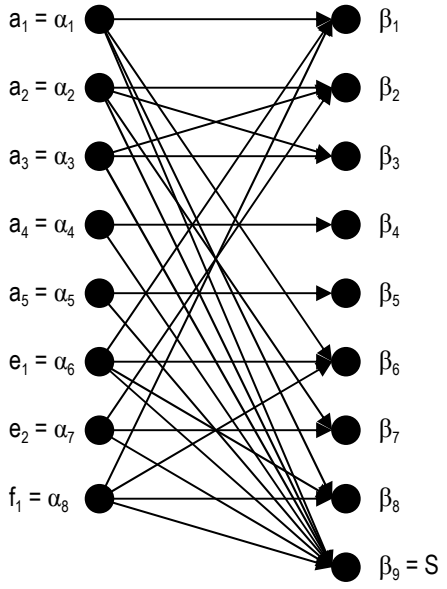
k on symbolin tunnusta z vastaava alkuperäisen osajoukon tunnus.

Hyödyntämistodennäköisyydet määritellään luvun 4.3.3 määritelmän 4.30 mukaisesti. Käytettävyystodennäköisyyksissä huomioitiin sekä havaitsemisen että hyödyntämisen todennäköisyys ja se lausuttiin yhtälön 4.31 mukaisesti. Edelleen saadaan kuvautumistodennäköisyydet perustuen määritelmään 4.32. Tällöin kanavamatriisiksi saadaan (sidottu kuvan 4.15 tilanteeseen):

$$C = \begin{pmatrix} c_{11} & 0 & 0 & 0 & 0 & c_{16} & 0 & c_{18} & c_{19} \\ 0 & c_{22} & c_{23} & 0 & 0 & 0 & c_{27} & 0 & c_{29} \\ 0 & c_{32} & c_{33} & 0 & 0 & 0 & 0 & 0 & c_{39} \\ 0 & 0 & 0 & c_{44} & 0 & 0 & 0 & 0 & c_{49} \\ 0 & 0 & 0 & 0 & c_{55} & 0 & 0 & 0 & c_{59} \\ c_{61} & 0 & 0 & 0 & 0 & c_{66} & 0 & c_{68} & c_{69} \\ 0 & c_{72} & 0 & 0 & 0 & 0 & c_{77} & 0 & c_{79} \\ c_{81} & 0 & 0 & 0 & 0 & c_{86} & 0 & c_{88} & c_{89} \end{pmatrix}$$

$$= \begin{pmatrix} P_{k1} & 0 & 0 & 0 & 0 & P_{K1} & 0 & P_{K1} & 1-3P_{K1} \\ 0 & P_{K2} & P_{K2} & 0 & 0 & 0 & P_{K2} & 0 & 1-3P_{K2} \\ 0 & P_{K3} & P_{K3} & 0 & 0 & 0 & 0 & 0 & 1-2P_{K3} \\ 0 & 0 & 0 & P_{K4} & 0 & 0 & 0 & 0 & 1-P_{K4} \\ 0 & 0 & 0 & 0 & P_{K5} & 0 & 0 & 0 & 1-P_{K5} \\ P_{K6} & 0 & 0 & 0 & 0 & P_{K6} & 0 & P_{K6} & 1-3P_{K6} \\ 0 & P_{K7} & 0 & 0 & 0 & 0 & P_{K7} & 0 & 1-2P_{K7} \\ P_{K8} & 0 & 0 & 0 & 0 & P_{K8} & 0 & P_{K8} & 1-3P_{K8} \end{pmatrix}. \qquad (4.45)$$

Symbolien kuvautumista kanavan yli voidaan havainnollistaa kuvan 4.16 mukaisesti. Erona luvussa 4.3.4 esitettyyn on se, että osa lähtöjoukon symboleista voi nyt kuvautua muiksikin tulojoukon symboleiksi kuin ”välilyönniksi”.



Kuva 4.16: Symbolien kuvautuminen kanavan yli, kun paikantaminen ei ole yksiselitteistä. Sidottu kuvan 4.15 tilanteeseen.

Tiedustelujärjestelmän suhteellinen kapasiteetti voidaan laskea luvussa 4.3.4 esitetyn yhtälön 4.34 mukaisesti. Ehdollista entropiaa ei kuitenkaan voida enää määrittää yhtälön 4.36 mukaisessa supistetussa muodossa, vaan se on laskettava yhtälöä 4.35 käyttäen.

Esimerkki 4.10

Tässä esimerkissä tarkastellaan hieman tarkemmin, miten kuvassa 4.15 esiintyvän symbolin a_1 kohdalla määräytyvät käytettävyystodennäköisyydet ja edelleen kuvautumistodennäköisyydet. Kuten esimerkissä 4.7, oletetaan tässäkin, että symbolin havaitsemistodennäköisyys on P_{H1} = 0.9. Kuvasta 4.15 näemme, että symbolin a_1 kanssa samaan lähetekategoriaan kuuluvat symboli e_1 ja f_1 sijaitsevat alle δ:n etäisyydellä symbolista a_1. Yhtälön 4.30 perusteella hyödyntämistodennäköisyydeksi saadaan nyt

$$P_{EX1} = \frac{1}{m_1} = \frac{1}{3} \approx 0.33.$$

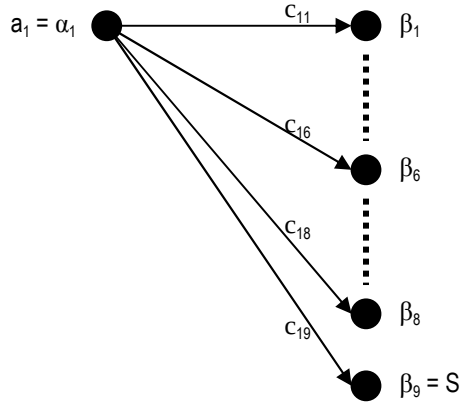
Käytettävyystodennäköisyydeksi saadaan yhtälön 4.31 perusteella

$$P_{K1} = P_{H1}P_{EX1} = 0.9 \cdot 0.33 = 0.297 \approx 0.3.$$

Merkitään lähtöjoukon symboleita seuraavasti: $a_1 = \alpha_1$, $e_1 = \alpha_6$ ja $f_1 = \alpha_8$. Näitä vastaavat tulojoukon symbolit ovat β_1, β_6 ja β_8. Tällöin on siis mahdollista, että $\alpha_1 \mapsto \beta_1$, $\alpha_1 \mapsto \beta_6$ ja $\alpha_1 \mapsto \beta_8$. Symbolin $a_1 = \alpha_1$ kuvautumista määrittelevä rivivektori matriisissa 4.45 saadaan nyt muotoon

$$c_{1j} = \begin{pmatrix} c_{11} & c_{12} & c_{13} & c_{14} & c_{15} & c_{16} & c_{17} & c_{18} & c_{19} \end{pmatrix} = \begin{pmatrix} 0.3 & 0 & 0 & 0 & 0 & 0.3 & 0 & 0.3 & 0.1 \end{pmatrix}.$$

Havainnollistetaan erikseen symbolin $a_1 = \alpha_1$ kuvautumista kanavan yli seuraavalla piirroksella 4.17.



Kuva 4.17: Symbolin $a_1 = \alpha_1$ kuvautuminen kanavan yli (otos kuvasta 4.16). ◇

Esimerkki 4.11

Tarkastellaan kuvien 4.15 ja 4.16 mukaista tilannetta, jossa toistensa kanssa limittyneistä symboleista on muodostettu uusi emissiomalli, jossa symboliavaruuden muodostaa joukko $\alpha = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6, \alpha_7, \alpha_8\}$. Liitteessä 6 esiteltyjen välivaiheiden jälkeen saadaan tiedustelujärjestelmän suhteelliseksi kapasiteetiksi $D_R = 1.7304 \frac{bit}{symboli}$ ja normalisoiduksi kapasiteetiksi

$$D_N = 1 - \frac{H(\alpha \mid \beta)}{H_s(\alpha)} = 1 - \frac{1.1199}{2.8494} = 0.607 .$$

Tiedustelujärjestelmän käytettävissä on siis noin 61 % mielenkiinnon kohteena olleella alueella tuotetusta informaatiosta. ◇

Esimerkit 4.7, 4.8 ja 4.9 ja 4.11 luovat selkeän kuvan siitä, miten olosuhteet vaikuttavat tiedustelijan ulottuville päätyvään informaation määrään. Selkeät mitalliset tulokset olosuhteiden välillä ovat myös nähtävillä.

4.4. Osajoukon aktiivisuuden arviointi suhteellisen entropian avulla

4.4.1. Jakaumien vertailu häiriöttömässä tilanteessa

Suhteellinen entropia tarjoaa keinon kahden todennäköisyysjakauman vertailulle. Jos oletetaan, että osajoukon emissiomalli tuottaa symboleita suljetun Markov ketjun tavoin, niin luvun 3.3.1 perusteella tiedämme, että on olemassa rajatodennäköisyydet μ_i, joita prosessi lähestyy. Prosessi on vakaa, kun symbolien jakauma noudattelee vakaata todennäköisyysjakaumaa μ. Tiedämme myös luvun 3.3.2 perusteella, että hetkellä n tuotettu todennäköisyysjakauma $\rho_n \to \mu$, kun $n \to \infty$. Voidaan ajatella, että eräs osajoukon elektronisen aktiivisuuden mittareista on se, kuinka nopeasti joukon emissiomalli saavuttaa tilannekuvan muodostamisen kannalta riittävän vakauden. Edelleen voidaan mieltää, että mitä hitaammin tuo vakautuminen tapahtuu, sitä epävarmempi on tiedustelijan tilannekuva kyseisestä osajoukosta, koska joukon tilastollinen luonne ei ole vakaa.

Olkoon ρ_h tiedustelutodennäköisyysjakauma, joka on muodostettu Markov prosessin tuottamien symbolien perusteella hetkellä h. Indeksiä h ei suoraan liitetä mitattavaan aikamääreeseen, vaan se tarkoittaa emissiomallin tuottamien symbolien lukumäärää. Indeksi voidaan si-

toa aikamääreisiin keskimääräisen symbolinopeuden φ_{avg} avulla. Luvun 3.2.6 perusteella tiedämme, että suhteellinen entropia on määritelty yhtälöllä 3.13. Tässä esitettyjä tarkasteluja varten määritellään suhteellinen entropia emissiomallin tuottamien symboleiden funktiona yhtälön 4.46 mukaisesti. Lisäksi vaaditaan, että todennäköisyysjakaumien ero saa olla korkeintaan ε, joka kuvaa sallitun epäsovituksen suuruutta.

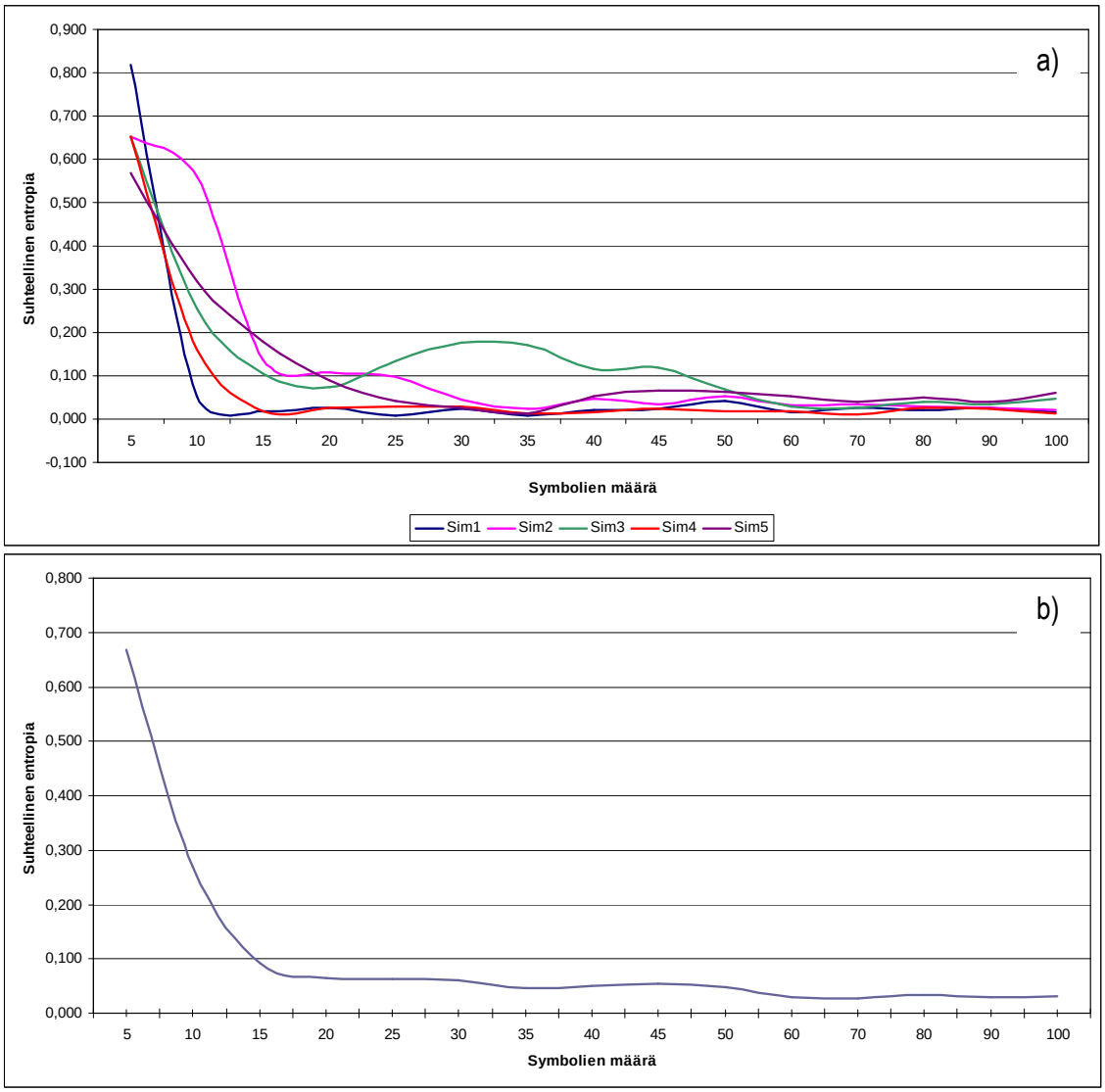
$$D_{KL}(h) = \sum_i \rho_{hi} \log_2 \frac{\rho_{hi}}{\mu_i} \leq \varepsilon \qquad (4.46)$$

Esimerkki 4.12

Oletetaan, että osajoukon emissiomalli noudattelee esimerkissä 4.5 ja kuvassa 4.7 esiteltyä yhden tilan omaavaa prosessia. Tällaisessa tilanteessa voidaan mieltää, että pitkällä aikavälillä prosessin vakaa todennäköisyysjakauma lähestyy kunkin symbolin tilastollista esiintymistodennäköisyyttä, ts. $\mu_i = p_i$. Olkoon siis vakaa todennäköisyysjakauma symboleille $a_1 – a_5$:

$$\mu = \begin{pmatrix} \mu_1 \\ \mu_2 \\ \mu_3 \\ \mu_4 \\ \mu_5 \end{pmatrix} = \begin{pmatrix} 0.143 \\ 0.143 \\ 0.143 \\ 0.143 \\ 0.428 \end{pmatrix}$$

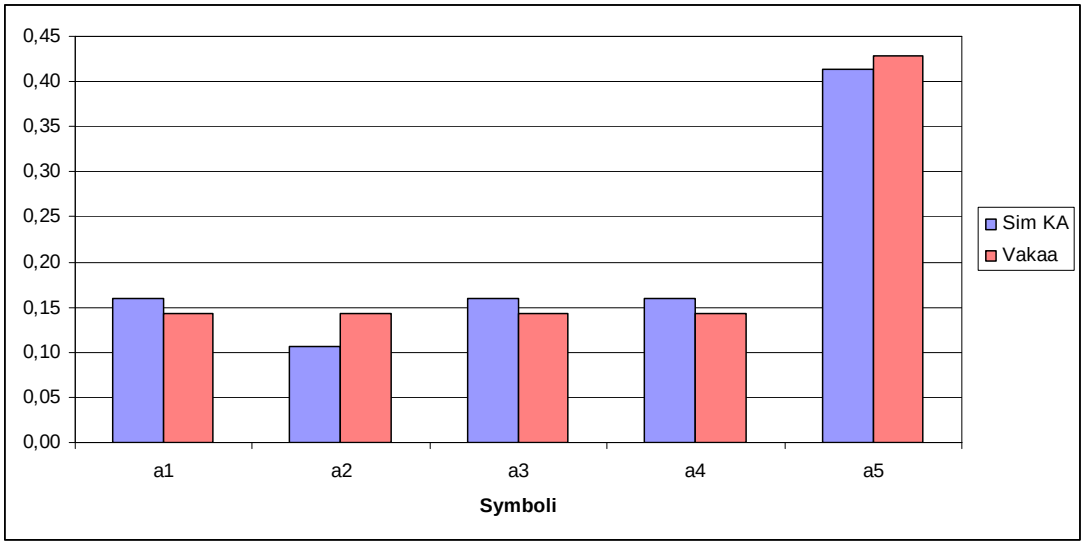
Yhtälöön 4.46 perustuen voidaan satunnaislukujen avulla pienimuotoisesti simuloida (ks. liite 7) suhteellisen entropian käyttäytymistä symbolien lukumäärän funktiona. Kuvassa 4.18 a on esitetty viiden simulaatiokierroksen tulokset sellaisenaan ja kuvassa 4.18 b näiden kierrosten keskiarvo. Tiedustelutodennäköisyysjakauma ρ_h on muodostettu, kun tuotettujen symbolien lukumäärä h = 5, 10, 15, 20, 25, 30, 35, 40, 45, 50, 60, 70, 80, 90, 100.



Kuva 4.18: a) Simulointikierrosten tulokset. b) Tulosten keskiarvo.

Seuraava luonnollinen kysymys on, mikä on sallitun epäsovituksen (ε) määrä, jota voidaan pitää hyväksyttävänä. Suhteellisen entropian yksikkö on bitti, mutta onko yllä olevaan esimerkkiin sitoen epäsovituksen mitta $D_{KL}(15) = 0.1$ bittiä paljon vai vähän? Jotta jonkinlainen perspektiivi käsillä olevaan ongelmaan kyetään rakentamaan, niin voimme pyrkiä hahmottamaan suurimman mahdollisen arvon, jonka suhteellinen entropia tässä tilanteessa saa. Tilastollisesti jakauma ρ_h on varmasti kauimpana jakaumasta μ, kun symbolien määrä $h = 1$ ja jos tämä on jokin symboleista a_1, a_2, a_3 tai a_4. Esimerkkitilanteessa suhteellinen entropia on tällöin $D_{KL}(1) = 2.81$ bittiä. Tähän verrattuna arvoa $D_{KL}(15) = 0.1$ voidaan pitää varsin pienenä. Yllä olevien kuvaajien perusteella havaitaan, että tämä arvo asettuu varsin sopivasti kohtaan, jonka jälkeen suhteellinen entropia vähenee enää vain varsin hitaasti. Seuraavaksi voidaan kysyä, miltä diskreetti jakauma ρ_{15} keskimäärin käytännössä näyttää verrattuna vakaaseen jakaumaan μ. Eli jos epäsovituksen raja-arvoksi valittiin $\varepsilon = 0.1$, niin miten selvästi emissiomallin tilastollinen rakenne tällöin paljastuu. Alla olevassa kuvassa 4.19 on esitetty viiden simulaatiokierroksen aikana tuotettujen jakaumien ρ_{15} keskimääräiset tulokset verrattuna vakaaseen jakaumaan μ.

Voidaan todeta, että osajoukon emissiomallin tilastollinen rakenne on jo selkeästi havaittavissa ja koska kuvan 4.18 b mukaisesti nähdään, suhteellinen entropia ei hetken h = 15 jälkeen enää ylitä arvoa 0.1, niin tilastollisen rakenteen luonne on yhä selvemmin havaittavissa, kun symbolien määrä kasvaa.



Kuva 4.19: Jakaumien ρ_{15} keskimääräinen jakauma verrattuna vakaaseen jakaumaan μ.

Viimeisenä kysymyksenä on: miten pitkään ajallisesti kestää ensimmäisestä havainnosta siihen, että sallittu epäsovitustaso on saavutettu? Tässä hyödynnetään emissiomallin keskimääräistä symbolinopeutta, joka tässä esimerkissä on φ_{avg} = 0.5. Nyt asetetaan

$$D_{KL}(t) = D_{KL}\left(\frac{h}{\varphi_{avg}}\right) = \varepsilon$$

Ja tämä saavutetaan $t = \frac{h}{\varphi_{avg}} = \frac{15}{0.5} = 30$ sekunnin kuluessa ensimmäisestä havainnosta[13]. ◇

Emissiomallin ergodisuus takaa sen, että ensimmäinen symboli (havainto) voidaan ottaa mistä tahansa symbolijonon kohdasta. Tilastollisesti ketju vakautuu tämän jälkeen aina ominaisuuksiensa mukaisesti riippumatta siitä, miten pitkään prosessi mahdollisesti on jo ollut käynnissä.

Yllä on todettu, että laskennallinen menetelmä riittävän vakaan todennäköisyysjakauman määrittämiseksi voidaan laatia suhteellisen entropian avulla. Menetelmän avulla voidaan arvioida, kuinka monta symbolia tiedustelija tarvitsee, jotta emissiomallin tilastollinen luonne on selvil-

[13] On muistettava, että tässä käsitellään edelleen häiriötöntä tilannetta, eli kaikki prosessin tuottamat symbolit ovat tiedustelijan käytössä. Myöskään erilaiseen automaattiseen tai manuaaliseen tiedon prosessointiin kuluvaa aikaa ei ole huomioitu.

lä. Kuitenkin yksiselitteisen ja yleisen raja-arvon (ε) määrääminen jakaumien sallitun epäsopivuuden mitaksi on vaikeaa eikä tähän problematiikkaan enempää tämän työn puitteissa keskitytä. Kun raja-arvo on kyetty määrittämään, on tämän jälkeen helppo arvioida kuinka pitkään ajallisesti kestää saavuttaa tuo raja-arvo. Näin ollen tämä laskennallinen menetelmä tarjoaa erään keinon arvioida kuinka nopeasti tiedustelijan tilannekuva saavuttaa riittävän tarkkuuden tai vaihtoehtoisesti arvioida saavutettua tarkkuutta käytössä olevan ajan funktiona. Vaikutusta tämän tarkkuuden kehittymiseen eri olosuhteissa voidaan tarkastella säätelemällä osajoukon elektronista aktiivisuutta kuvaavaa emissiomallia.

4.4.2. Jakaumien vertailu häiriöllisessä tilanteessa

Luvussa 4.4.1 on esitelty, miten suhteellista entropiaa voidaan hyödyntää arvioitaessa, miten nopeasti tiedustelijan tilannekuva on tilastollisesti riittävän tarkka. Menetelmä perustuu lausekkeen 4.46 laskennalliseen hyödyntämiseen.

Häiriöllisessä tilanteessa vakaa jakauma μ on määritelty samoin, kuin häiriöttömässä tilanteessa. Myös vertailujakauman ρ_h määrittely on sama, mutta sen muodostamisessa on nyt huomioitava se, että osa symboleista häviää kohinan ja häiriöiden vaikutuksesta. Käytännössä tämä tarkoittaa sitä, että tiedustelija tekee tilannekuvaansa perustuen symbolijonoon, jonka todennäköisyysjakauma voidaan määritellä

$$\rho_{Dj} = \frac{h_j}{h - h_{n+1}} = \frac{h_j}{\sum_{j=1}^{n+1} h_j - h_{n+1}} = \frac{h_j}{\sum_{j=1}^{n} h_j}, \qquad (4.47)$$

missä $j = 1, 2, \ldots, n$

h_j = onnistuneesti vastaanotettujen symbolien b_j lukumäärä

h_{n+1} = vastaanottamattomien symbolien lukumäärä (”välilyönnit”)

h = tuotettujen symbolien lukumäärä.

Nyt summa $\sum_{j=1}^{n} h_j = d$ on tiedustelijan onnistuneesti vastaanottamien symbolien kokonaislukumäärä ja yllä esitelty tiedustelutodennäköisyysjakauma ρ_D voidaan lausua

$$\rho_{Dj} = \frac{h_j}{d}, \qquad j = 1, 2, \ldots, n. \qquad (4.48)$$

Tilanteesta riippuen tämä todennäköisyysjakauma saattaa poiketa merkittävästi vakaasta jakaumasta. Suhteellinen entropia voidaan edelleen määrittää emissiomallin tuottamien symboleiden lukumäärän funktiona, mutta vertailujakaumana toimii tiedustelutodennäköisyysjakauma, jossa ei siis ole huomioitu vastaanottamatta jääneitä symboleita. Suhteellinen entropia voidaan nyt ilmaista

$$D_{KL}(h) = \sum_j \rho_{Dj}(h) \log_2 \frac{\rho_{Dj}(h)}{\mu_j}. \qquad (4.49)$$

Esimerkiksi laskennallisesti simuloitaessa häiriöllistä tilannetta, on huomioitava, että symbolit on tuotettava vastaanottojakauman mukaisesti, koska tämä jakauma määrittää, millainen osuus lähetetyistä symboleista häviää.

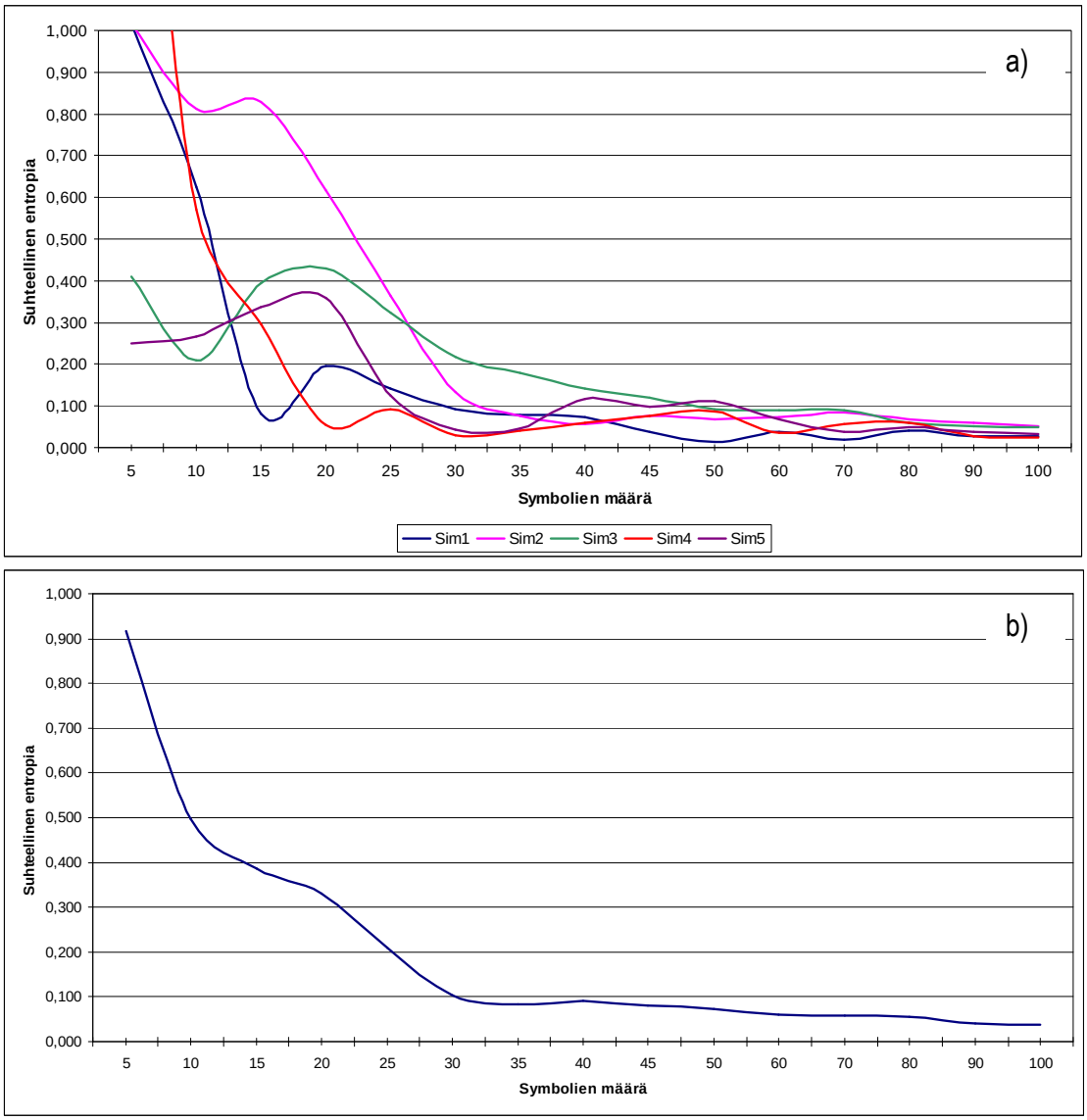
Esimerkki 4.13

Käytetään samaa emissioympäristöä, kuin häiriöttömässä tapauksessa (luku 4.4.1) ja jolle on määritelty häiriöiden vaikutus esimerkissä 4.7. Simuloitaessa emissioympäristöä, muodostetaan symbolit alla olevan vastaanottojakauman mukaisesti

$$v = \begin{pmatrix} v_1 & v_2 & v_3 & v_4 & v_5 & v_6 \end{pmatrix} = \begin{pmatrix} 0.129 & 0.129 & 0.129 & 0.129 & 0.300 & 0.186 \end{pmatrix},$$

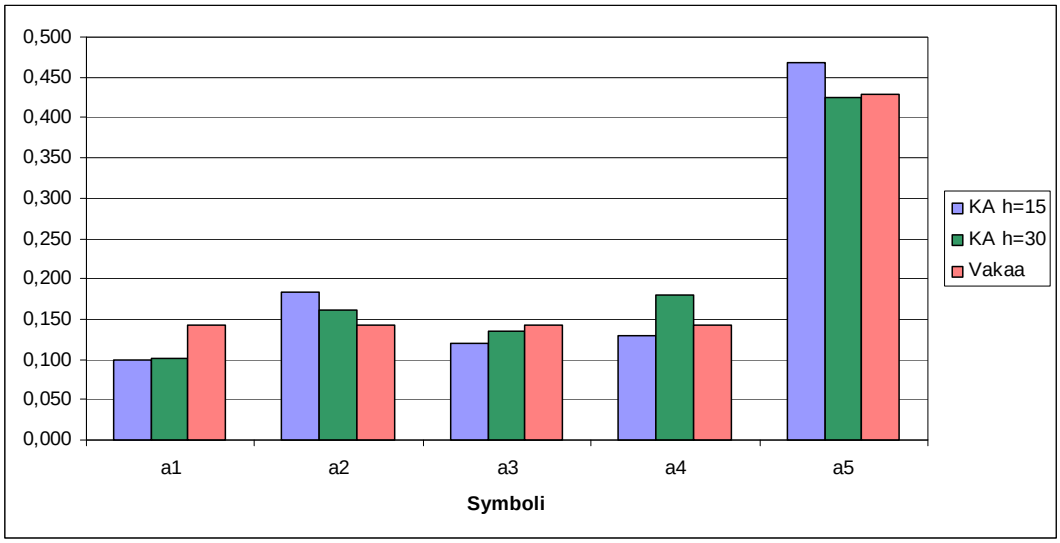
missä $v_6 = 0.186$ edustaa vastaanottamatta jäävien symboleiden osuutta.

Vakaana jakaumana μ toimii edelleen häiriöttömässä tilanteessa esitelty jakauma ja vertailujakauma ρ_D muodostetaan yllä esiteltyjen lausekkeiden 4.47 ja 4.48 mukaisesti.. Laskettaessa suhteellinen entropia kanavalle tuotettujen symboleiden funktiona, saadaan kuvissa 4.20 a ja b esitetyt kuvaajat.



Kuva 4.20: a) Erillisten simulaatiokierrosten tulokset b) Simulaatioiden keskiarvo.

Vertailemalla häiriöttömän ja häiriöllisen tilanteen tuloksia havaitaan, että häiriöllisessä tilanteessa suhteellisen entropian D_{KL} = 0.1 bit saavuttaminen vaatii kaksinkertaisen määrän symboleita häiriöttömään tilanteeseen verrattuna. Nähdään myös, että pienillä symbolimäärillä eri simulaatiokierrosten hajonta on varsin suurta. Kuvassa 4.21 on esitetty keskimääräiset symbolien jakaumat tilanteissa h = 15 ja h = 30. Kuvasta voidaan todeta, että jo varsin alhaisella lähetettyjen symbolien määrällä tilastollinen jakauma on kohtuullisen selkeä. On kuitenkin huomioitava, että tämä esitystapa ei ota kantaa keskihajontaan, joka on selkeästi varsin suurta kuvan 4.20 a perusteella.



Kuva 4.21: Symboleiden keskimääräiset jakaumat, kun lähetettyjen symboleiden määrä on 15 ja 30. ◇

Esiteltyjen esimerkkien tarkoituksena ei varsinaisesti ole tehdä johtopäätöksiä siitä, miten paljon olosuhteiden vaikutus muuttaa tiedustelijan tilannekuvan muodostamista. Kuitenkin nämäkin esimerkit osoittavat, että selkeitä eroavaisuuksia voidaan nähdä eri tilanteissa. Näin ollen esiteltyä menetelmää voidaan hyödyntää osajoukon elektronista aktiivisuutta ja elektronisten suojautumisen toimenpiteiden vaikutusta arvioitaessa. Jakaumien vertailuun perustuva elektronisen aktiivisuuden arvioinnin eräänä vahvuutena on se, että haluttaessa voidaan arvioida aikaan sitoen, kuinka pitkään riittävän hyvän tilastollisen tilannekuvan rakentaminen kestää. Tämä arvio saadaan suoraan laskettua, kun tiedetään emissioympäristön tuottamien symbolien keskimääräinen symbolinopeus. On myös mahdollista testata, miten symbolinopeuden muutos vaikuttaa tilastollisen tilannekuvan muodostumiseen. Aikaan sidotuissa arvioissa on muistettava se, että tässä esitetty menetelmä ei suoraan huomioi tiedustelujärjestelmän tiedonkäsittelyviiveitä. Mikäli vastaanotettujen lähetteiden käsittely vaatii ajallisesti huomattavan määrän työtä itse tiedustelujärjestelmässä, saattavat nämä vaikuttaa merkittävästi myös aikaarvioihin. Prosessoinnin nopeuteen vaikuttaa huomattavasti se, tuleeko tiedustelujärjestelmän operaattorin manuaalisesti raportoida tehdyistä havainnoista sekä se, joudutaanko havainto analysoimaan manuaalisesti esimerkiksi kuuntelemalla nauhoite vastaanotetusta datasta [53, s. 458]. Poisel on simulaatioihin perustuen esittänyt, että onnistunut tiedustelutoiminta liikennetiheytensä puolesta rajoitetussa emissioympäristössä edellyttää havaintokohtaisen käsittelyajan rajoittumista 20 – 100 sekuntiin [53, s. 458]. Todettakoon vielä Kuusiston [39, s. 174] artikkelissaan esittäneen, että automaattisella tiedustelujärjestelmällä kyetään vähän kohteita sisältävästä emissioympäristöstä tuottamaan reaaliaikaista tilannekuvaa muutamien minuuttien toiminnan jälkeen, mikäli kohteet ovat hyvin aktiivisia. Vastaavasti tiheässä emissioympäristössä kohtuullisen tilannekuvan muodostamiseen kyetään alle kahdessa tunnissa [39, s. 174].

5. JOUKON ELEKTRONISEN AKTIIVISUUDEN ARVIOIMINEN JA MENETELMIEN KÄYTETTÄVYYDEN KATSELMOINTI

5.1. Tunnistaminen

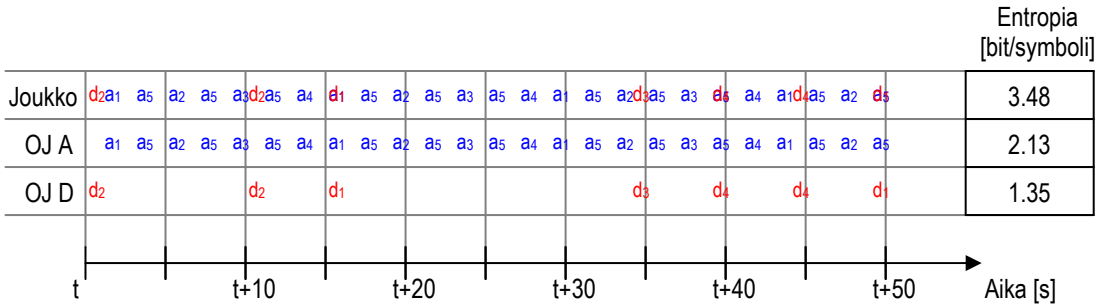
Luvussa 4.2.2 käsiteltiin erityisesti osajoukon tunnistettavuutta lähetetodennäköisyyksiin perustuen. Toisin sanoen arvioitiin osajoukon tilastollista erottuvuutta muista osajoukoista ja koko joukosta lähetteiden yleisyyteen tai harvinaisuuteen pohjautuen. Esitelty menetelmä sisältää myös koko joukkoa käsittelevät analyysit, joten erillistä tarkastelua koko joukon osalta ei ole tarvetta tehdä.

Kriittisen toiminnan tunnistettavuutta käsiteltiin luvussa 4.2.3. Esitettyä tarkastelua ei käytännössä ole mielekästä tehdä joukolle, joka ei ole osa jotain suurempaa kokonaisuutta; pyritäänhän nimenomaisesti hahmottamaan, miten hyvin jokin toiminta erottuu ympäristöstään. Näin ollen tarkastelut eri tasoilla on tehtävä osana sopivasti valittua suurempaa kokonaisuutta luvussa 4.2.3 esiteltyjä periaatteita noudattaen. Erillinen lisätarkastelu tässä yhteydessä on näin ollen turha.

5.2. Joukon aktiivisuuden arviointi entropian ja yhtenäisinformaation avulla

5.2.1. Joukon emissiomalli ja entropia

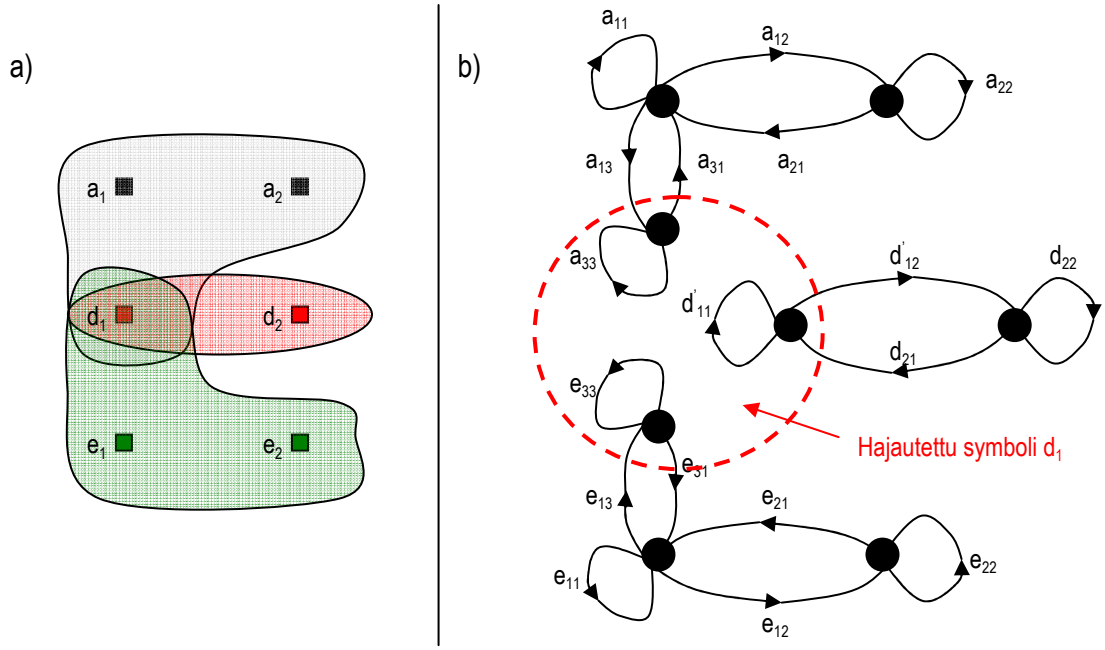
Yksinkertaisimmassa tilanteessa osajoukkojen emissiomallit ovat toisistaan riippumattomia rinnakkaisia prosesseja. Tällöin ei tarvitse erikseen rakentaa emissiomallia koko joukolle, vaan joukon tuottama symbolijono voidaan mieltää erillisten osajoukkojen symbolijonojen yhdistelmäksi. Koska osajoukkojen emissioympäristöt ovat riippumattomia, saadaan koko joukon entropia määritettyä suoraan osajoukkojen entropioiden summana. Kuvassa 5.1 on esimerkki tilanteesta, jossa joukon oletetaan muodostuneen kahdesta riippumattomasta osajoukosta.



Kuva 5.1: Riippumattomien osajoukkojen A ja D tuottamat symbolijonot ja niiden yhteistuloksena aikaansaatu koko joukon symbolijono. Koko joukon entropia on osajoukkojen entropioiden summa. Osajoukkojen A ja D ominaisuudet esimerkissä 4.5 esitetynlaiset.

Tarkasteltaessa koko joukon informaation määrää on muistettava entropian yhteenlaskettavuuden määritelmä (ks. luku 3.2.2), jossa nimenomaisesti korostuu yhteistapahtuman AD todennäköisyysjakauma ja sen avulla muodostunut entropia. Paras tapa käsitellä yhteenlasketun informaation määrää on mieltää se entropian määräksi per symboli (bit/symboli). Tällöin osajoukkojen entropioiden yhteenlasku antaa automaattisesti oikean tuloksen. Tilanne ei ole aivan yhtä selkeä sidottaessa informaation määrä aikaan. Tällöin erillisten osajoukkojen entropioiden yhteenlasku ei suoraan anna oikeaa tulosta, koska symbolikohtaisesti ei ole huomioitu yhteistapahtuman AD tuottaman epävarmuuden lisääntynyttä määrää. Tilanteesta on esitetty esimerkki liitteessä 8.

Mikäli osajoukkojen emissiomallien käyttökelpoisuus edellyttää jonkin usealle osajoukolle yhteisen symbolin (lähetteen) sisällyttämistä useisiin eri osajoukkoihin, voidaan tämä toteuttaa hajauttamalla yhteinen symboli oikeassa suhteessa osajoukkojen emissiomallien kesken. Oikeastaan tämä tarkoittaa, että alun alkaen on olemassa stokastisen prosessin tila, joka tuottaa alkuperäistä symbolia tiettyjen ominaisuuksien perusteella ja tämä tila jaetaan osatiloiksi, joilla on kutakin osajoukkoa vastaavat ominaisuudet. Tavoitteena on edelleen pitää osajoukkojen emissiomallit toisistaan riippumattomina, jotta informaation yhteenlaskettavuus koko joukon osalta pätisi. Kuvissa 5.2 a ja b on esitetty symbolin hajauttamisen periaate.



Kuva 5.2: a) Emissioympäristö, joka koostuu kolmesta osajoukosta, joilla kaikilla yhteisenä symbolina d_1. b) Emissioympäristöstä muodostetut erilliset emissiomallit. Symbolia d_1 vastaava tila on hajautettu osatiloiksi, joita vastaavat symbolit a_3, d'_1 ja e_3.

Hajautettavan tilan ominaisuudet on jaettava oikeassa suhteessa kullekin osatilalle. Erityisesti on tunnettava kuinka usein hajautettavaa symbolia kuvaava tila tuottaa symbolin, joka voidaan liittää osaksi kutakin osajoukon emissiomallia. Jos oletetaan, että alkuperäinen symboli g_0 jaetaan osasymboleiksi g_1, g_2, …, g_n eli toisin sanoen symbolia g_0 vastaava prosessin tila jaetaan osatiloiksi, jotka vastaavat symboleita g_1, g_2, …, g_n, niin tällöin alkuperäistä tilaa vastaava symbolinopeus φ_0 on osatilojen symbolinopeuksien keskiarvo. Pätee siis

$$\varphi_0 = \frac{\sum_{i=1}^{n} \varphi_i}{n}, \qquad (5.1)$$

missä φ_i on kutakin osatilaa vastaava symbolinopeus.

Osatilojen symbolinopeuksien lisäksi on tiedettävä jokaisen osatilan tuottamien symbolien tilastollinen jakauma suhteessa osajoukon muihin symboleihin. Tällöin voidaan määrittää tarvittavat siirtymätodennäköisyydet. Tämän jälkeen osajoukon emissiomallia voidaan käsitellä ja hyödyntää kuten edellä luvuissa 4.3.1 ja 4.3.2 on esitetty. Koska osajoukot ovat edelleen riippumattomia toisistaan, voidaan koko joukon mallinnus ja entropia määritellä tämän luvun alussa esitellyllä tavalla.

5.2.2. Tiedustelujärjestelmän kapasiteetti suhteessa koko joukkoon

Tiedustelujärjestelmän suhteellista kapasiteettia verrattuna yksittäiseen osajoukkoon käsiteltiin luvussa 4.3.4. Todettiin, että tiedustelujärjestelmän suhteellinen kapasiteetti voidaan mieltää yhtenäisinformaatioksi tiedustelujärjestelmän vastaanottaman informaation ja emissioympäristön tuottaman informaation välillä. Lisäksi osoitettiin, että symboleiden sieppaamiseen, ilmaisuun ja hyödynnettävyyteen liittyvät tekijät voidaan huomioida esitetyssä informaatioteoreettisessa menetelmässä.

Tiedustelujärjestelmän suhteellisen kapasiteetin määrittäminen koko joukon suhteen perustuu edellä esitettyihin riippumattomiin osajoukkoihin. Yhtenäisinformaatio lasketaan erikseen jokaiselle osajoukolle jolloin myös ne ovat toisistaan riippumattomia. Luvussa 4.2.3 ja liitteessä 1 osoitettiin, että toisistaan riippumattomat yhtenäisinformaatiot voidaan laskea yhteen ja lopputuloksena saadaan koko joukkoa kuvaava informaatiosuure, joka tässä tapauksessa on tiedustelujärjestelmän suhteellinen kapasiteetti.

Kuvautumistodennäköisyydet määritetään erikseen jokaiselle joukon osajoukolle luvun 4.3.3 periaatteita noudattaen. Usealle osajoukolle yhteisen symbolin jakaminen osasymboleiksi luvun 5.2.1 mukaisesti ei sinänsä vaikuta kuvautumistodennäköisyyksien muodostumiseen.

Esimerkki 5.1

Oletetaan, että joukko koostuu kahdesta osajoukosta A ja D. Osajoukkojen ominaisuudet vastaavat esimerkissä 4.5 esiteltyjä vastaavia osajoukkoja. Lisäksi oletetaan, että symbolit a_1 ja d_1 tuottavat vain ”välilyöntejä” (ovat radiohiljaisuudessa). Osajoukon A kuvautumistodennäköisyydet ovat samat kuin esimerkissä 4.8. Osajoukon D osalta oletetaan, että havaitsemistodennäköisyys on symboleiden d_2, d_3 ja d_4 kohdalla 0.8. Hyödyntämistodennäköisyyksiä ei huomioida kummankaan osajoukon osalta. Määriteltäessä tiedustelujärjestelmän suhteellinen kapasiteetti osajoukoille ja koko joukolle, saadaan yhteenvedoksi taulukossa 5.1 esitetyt tulokset. Osajoukon A tarkastelu on vastaava, kuin on esitetty esimerkissä 4.8. Osajoukon D osalta yksityiskohtaiset laskelmat on esitetty liitteessä 9.

	Entropia H_s	Tied.järj. suht. kapasiteetti D_R	Ehdollinen entropia	Prosenttia D_R/H_s
Osajoukko A	2.13	1.61	0.52	75.6 %
Osajoukko D	1.35	0.74	0.61	54.5 %
Koko joukko	3.48	2.35	1.13	67.5 %

Taulukko 5.1: Tiedustelujärjestelmän suhteellisen kapasiteetin määrittäminen joukolle informaation yhteenlaskettavuuteen perustuen.

Taulukosta havaitaan, että noin 68 % koko joukon tuottamasta informaatiosta on tiedustelujärjestelmän saatavilla. Osajoukkojen A ja D välinen elektronisen suojautumisen tason on suhteessa niiden tuottamaan informaatioon nähden kohtuullisen suuri (n. 20 %) osajoukon D eduksi. Absoluuttisesti osajoukon D etu on kuitenkin vain 0.09 bit/symboli (ehdollisten entropioiden perusteella). ◇

Yllä oleva esimerkki havainnollistaa, että informaation yhteenlaskettavuus tarjoaa varsin yksinkertaisen keinon käsitellä tarvittaessa suuriakin joukkokokonaisuuksia, kunhan osajoukot pidetään toisistaan riippumattomina.

5.3. Joukon aktiivisuuden arviointi suhteellisen entropian avulla

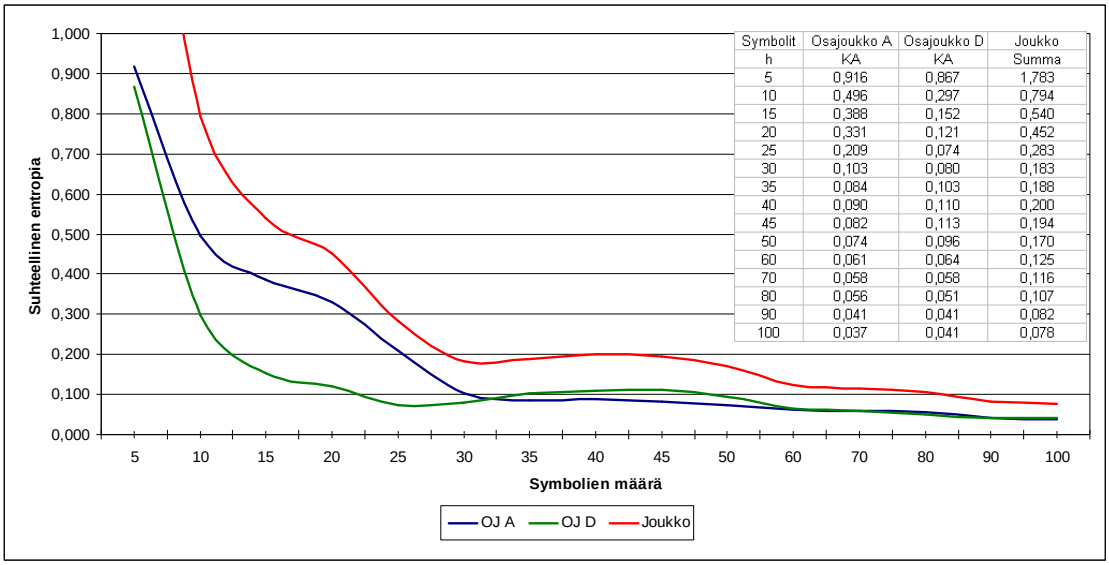
Osajoukkoja käsiteltäessä lähtökohtana oli oletus, että suhteellinen entropia on eräs tapa arvioida tiedustelijan luoman tilannekuvan laatua. Tarkasteltaessa suhteellista entropiaa tuotettujen symboleiden (lähetteiden) funktiona voidaan muodostaa käsitys siitä, miten tarkka tilannekuva tilastollisesti on. Tilannekuva koko joukosta muodostuu sen osajoukkojen kautta. Oletettaessa osajoukot tilastollisesti toisistaan riippumattomiksi, voidaan myös suhteellisen entropian kohdalla hyödyntää informaation yhteenlaskettavuutta [36]. Näin ollen koko joukon suhteellinen entropia määritetään osajoukkojen entropioiden summana. Jos siis osajoukkoa A vastaa tiedustelutodennäköisyysjakauma $\rho_D^A = (\rho_1^A, ..., \rho_m^A)$ jota vertaillaan vakaaseen todennäköisyysjakaumaan $\mu^A = (\mu_1^A, ..., \mu_m^A)$ ja osajoukkoa B vastaa tiedustelutodennäköisyysjakauma $\rho_D^B = (\rho_1^B, ..., \rho_n^B)$ jota vertaillaan vakaaseen todennäköisyysjakaumaan $\mu^B = (\mu_1^B, ..., \mu_n^B)$, niin tällöin näiden osajoukkojen muodostaman joukon suhteellinen entropia on (ks. esim. [1, s. 201], [36], [37, s. 12 - 13]):

$$D_{KL}(\rho_D^A \rho_D^B \parallel \mu^A \mu^B) = D_{KL}(\rho_D^A \parallel \mu^A) + D_{KL}(\rho_D^B \parallel \mu^B). \qquad (5.2)$$

Esimerkki 5.2

Joukko koostuu osajoukoista A ja D, joiden ominaisuudet ovat esimerkin 4.5 mukaiset (ks. myös liite 3). Oletetaan, että symbolit $a_1, a_2, a_3, a_4 \in A$ kuvautuvat oikein todennäköisyydellä 0.9 ja symboli $a_5 \in A$ kuvautuu oikein todennäköisyydellä 0.7. Symbolit $d_1, d_2, d_3, d_4 \in D$ kuvautuvat oikein todennäköisyydellä 0.8. Symbolit, jotka eivät kuvaudu oikein, menetetään. Lasketaan kummallekin osajoukolle suhteellinen entropia symboleiden lukumäärän funktiona (ks. luku 4.4.2). Koko joukon suhteellinen entropia saadaan yhtälön 5.2

mukaisesti. Tulokset voidaan esittää kuvan 5.3 mukaisesti. Osajoukkojen käyrät perustuvat numeeristen simulointikierrosten keskiarvoisiin tuloksiin.



Kuva 5.3: Joukon ja sen osajoukkojen suhteelliset entropiat symbolien lukumäärän funktiona. Osajoukkojen kuvaajat perustuvat simulointeihin. Joukon kuvaaja saadaan osajoukkojen summana.

Yllä esitetynlaisista kuvaajista on eroteltavissa osajoukot, joiden tilastollinen rakenne on joko helposti tai suhteellisen vaikeasti selvitettävissä. On kuitenkin huomattava, että tällainen esitystapa ei kerro koko totuutta tilanteesta, koska osajoukot tuottavat symboleita erilaisilla symbolinopeuksilla ja tätä ei ole yllä huomioitu. Jos yllä olevassa tilanteessa tavoitellaan suhteellisen entropian arvoa 0.1, niin tämä arvo saavutetaan taulukossa 5.2 esiteltyjen aikojen kuluessa. Tarvittaessa erilaisille emissiomalleille on helppo laatia käyrästöt, joista on nähtävissä, kuinka kauan tietyn symbolimäärän saavuttaminen kestää. On syytä muistaa, että tällaiset käyrästöt on laadittava uudestaan aina, jos emissiomallissa tapahtuu muutoksia; esimerkiksi ”välilyöntien” määrä lisääntyy elektronisen suojautumisen toimenpiteiden ansiosta.

	Symbolien lkm noin [kpl]	Symbolinopeus [symb/sek]	Vaadittu aika [sek]
Osajoukko A	30	0.5	60
Osajoukko D	22	0.14	157
Joukko	82	0.64	128

Taulukko 5.2: Vaaditut symbolien lukumäärät ja ajat suhteellisen entropian arvon 0.1 saavuttamiseksi.

Kuten taulukosta huomataan, osajoukon D kohdalla vaaditaan noin 2½-kertainen aika vaaditun kriteerin täyttämiseksi verrattuna osajoukkoon A. Tämä ei ole selkeästi nähtävissä kuvasta 5.3. Tarkastelut on siis aina sidottava myös aikaan. Koko joukon kohdalla vaadittuun kriteeriin pääseminen edellyttää varsin suurta symbolimäärää verrattuna osajoukkoihin. Toisaalta, jos koko joukon kriteeri lasketaan arvoon 0.2, niin tällöin riittää hieman alle 30 symbolia. Ku-

ten jo aikaisemmin mainittua, tässä työssä ei pyritä etsimään suositeltavia yleisiä arvoja jakaumien epäsovituksille. ◇

5.4. Menetelmien käytettävyyden arviointia

5.4.1. Hyödynnettävyys elektronisen suojautumisen keinoja arvioitaessa

Luvuissa 4 ja 5 on kuvattu neljä menetelmää, joita voidaan hyödyntää elektronisen aktiivisuuden ja elektronisen suojautumisen arvioimisessa. Kuvatut menetelmät ovat:

- Menetelmä 1: Joukon lähetejakauman analyysi (luku 4.2.2)
- Menetelmä 2: Kriittisen toiminnan tunnistaminen (luku 4.2.3)
- Menetelmä 3: Tiedustelujärjestelmän ulottuville päätyvän informaation määrän arviointi (luvut 4.3 ja 5.2)
- Menetelmä 4: Tilannekuvan tarkkuuden arviointi suhteellisen entropian avulla (luvut 4.4 ja 5.3).

Seuraavassa on arvioitu näiden menetelmien hyödynnettävyyttä analysoitaessa erilaisia elektronisen suojautumisen teknisiä, toiminnallisia ja taktisia menetelmiä. Tarkastellut suojautumisen menetelmät ovat luvun 2.2.3 taulukossa 2.1 esitetyn mukaisia.

Kuten taulukosta 5.3 nähdään, ovat menetelmät 1 ja 2 nimenomaisesti laadittu tukemaan joukon laitteistojen ja lähetteiden identtisyyden analysointia. Joukon liikkeen vaikutusta kriittisen toiminnan tunnistamiselle voidaan myös tarkastella menetelmän 2 avulla. Tällainen tarkastelu kuitenkin vaatii kriittiseen toimintaan osallistuvien joukkojen ja muiden samalla alueella toimivien joukkojen liikkeen mallintamista jollain menetelmällä.

Menetelmien 3 ja 4 hyödyntämiskohde on erityisesti erilaisten emissioiden hallintaan liittyvien rajoitusten tai sallittujen toimintojen testaaminen näkökulmasta, jossa arvioidaan tiedustelijan ulottuville joutuvan informaation määrää ja muodostetun tilannekuvan tarkkuutta. Emissioiden hallinnan alle luetaan myös elektronisen aktiivisuuden mahdollisimman tasainen jakautuminen eri lähettimien kesken. Tällöin tilastollisen liikenneanalyysin tekeminen kerätystä informaatiosta on kaikkein vaikeinta. Menetelmillä 3 ja 4 voidaan arvioida myös elektronisen aktiivisuuden jakautumisen vaikutuksia informaation määriin.

Suojautumisen menetelmä ja kuvaus	Informaatioteoreettiset menetelmät			
	1	2	3	4
LPI ja LPD tekniikat Menetelmillä pyritään vaikeuttamaan signaalin sieppaamista ja ilmaisua. Esimerkkeinä taajuus hypytys ja suorasekvenssitekniikat.	-	-	E	E
Viestiliikenteen salaaminen - Datan tekninen salaaminen salausalgoritmeilla - Viestiliikennekuri ml. peitteistöjen käyttö	-	-	-	-
Toimintaparametrien säätely Esimerkiksi lähetystehojen optimointi, modulointitavat ja lähetteiden polarisaatiot sekä niiden muutokset.	-	-	E	E
Maskaus Elektronisen tiedustelujärjestelmän aktiivinen häirintä siten, että omia hyötylähetteitä ei kyetä havaitsemaan.	-	-	E	E
Laitteistojen ja lähetteiden identtisyys Erilaisten joukkojen varustaminen identtisellä kalustolla vaikeuttaa tiedustelijan johtopäätösten tekoa.	S	S	-	-
Maaston hyväksikäyttö Esimerkiksi tiedustelun vaikeuttaminen maastoesteitä hyödyntämällä. Toiminnallinen menetelmä käsiteltäessä yksittäisen laitteen käyttöperiaatteita. Taktinen menetelmä otettaessa huomioon sotilasjoukon operaatiossa.	-	-	S	S
Suunta-antennit Suuntaamalla teho kapealle sektorille on mahdollista vaikeuttaa signaalin havaitsemista olettaen, että tiedustelusensori ei sijaitse pääkeilan suunnassa. Voidaan mieltää myös taktisen tasan menetelmäksi, mikäli huomioidaan esim. sotilasjoukon viestisuunnitelmien teossa.	-	-	E	E
Liike Joukkojen ja järjestelmien liikkeellä hidastetaan tiedustelutoimintaa, koska tiedustelija joutuu uhraamaan yhä uudestaan resursseja saman asian analysoimiseksi.	-	S	S	S
Emissioiden hallinta (EMCON, Emission Control) Säätelemällä joukkojen ja järjestelmien emissioita ajallisesti, alueellisesti ja toimintaan liittyen pyritään estämään tai vaikeuttamaan tiedustelijan työtä. Emissioiden hallintaan oletetaan kuuluvan myös taajuushallinnan ja laitteiden tahattomasti vuotavan säteilyn hallinnan.	-	-	S	S
Harhauttaminen Harhauttavilla toimilla annetaan väärä kuva esim. omasta ryhmityksestä ja toiminnasta. Tällä vaikeutetaan oikean tilannekuvan muodostamista. Joskus tämän tyyppinen harhauttaminen asetetaan elektronisen vaikuttamisen alaisuuteen. Tässä sitä käsitellään kuitenkin elektronisen suojautumisen elementtinä.	E	E	E	E

Taulukko 5.3: Informaatioteoreettisten menetelmien soveltuvuus erilaisten elektronisen suojautumisen keinojen analysointiin. S = soveltuu, E = soveltuu epäsuorasti, - = ei sovellu.

Samaisia menetelmiä voidaan hyödyntää myös arvioitaessa esimerkiksi joukon tai osajoukon taktisia toimintavaihtoehtoja. Menetelmien avulla voidaan vertailla joukon liikkeen ja maantieteellisen suuntautumisen vaikutuksia tiedustelijan ulottuville päätyvään informaatioon nähden. Tällöin voidaan laatia mitallisia suosituksia eri vaihtoehdoille elektronisen suojautumisen osalta. Maastoon sidotut tarkastelut voidaan toteuttaa hyödyntämällä rinnalla jotain radioaalto-

jen etenemistä mallintavaa ohjelmistoa, jolloin signaalin ilmaisuun liittyvä mallinnus on tarkinta.

Menetelmiä 3 ja 4 voidaan epäsuorasti hyödyntää kaikkien niiden elektronisen suojautumisen menetelmien arvioinnissa, jotka vaikeuttavat lähetteiden havaitsemista (sieppaamista tai ilmaisua). Tämä kuitenkin edellyttää, että suojautumiskeinojen vaikutukset kuvautumistodennäköisyyksiin kyetään jollain tapaa määrittelemään.

Kaikilla esitellyillä menetelmillä voidaan tukea harhauttavan toiminnan suunnittelua. Elektronisen aktiivisuuden kuvaaminen liittyy oleellisesti toimintaan, jossa halutaan kuvata joukon toimintaa harhautustarkoituksessa. Menetelmien 1 ja 2 avulla voidaan arvioida, miten hyvin harhauttavan osaston lähettimet vastaavat jakaumaltaan sitä joukkoa, jota halutaan kuvata. Menetelmillä 3 ja 4 voidaan arvioida millainen tulee harhauttavan joukon elektronisen aktiivisuuden tason olla, jotta tiedustelijan saatavilla on informaatiomäärä, joka vastaa harhautuksella kuvattavaa joukkoa. Käytännössä tähän tehtävään vastaa parhaiten hyvin rakennettu emissiomalli. Jos jollekin osajoukolle on kyetty määrittämään malli, joka vastaa osajoukon elektronista aktiivisuutta jossain tietyssä toiminnassa, niin tällöin emissiomalli toimii suoraan ohjenuorana harhauttavan osaston lähettimien käytölle.

Informaatioteoreettiset menetelmät tarjoavat mahdollisuuden uudenlaiseen joukkokohtaiseen EMCON-ohjeistukseen, joka pohjautuu tiedustelijan ulottuville tuotettavan informaation määrään. Toisin sanoen kriteerit erilaisille EMCON-tasoille voidaan asettaa perustuen yhtenäisinformaation suhteelliseen osuuteen koko joukon/osajoukon tuottamasta informaatiosta (entropiasta). Kiinnityspisteenä voi toimia tyypillistä taistelutilannetta kuvaavan emissiomallin E_E tuottama entropia H_{sE} (ks. luku 4.3.2), joka siis vastaa tilannetta, jossa informaatiota saadaan tuottaa 100 % intensiteetillä. Asettamalla vaatimukset erilaisille suojautumisen tasoille esimerkiksi prosentteina suhteessa entropiaan H_{sE}, voidaan esiteltyjen menetelmien perusteella arvioida millaisia ehtoja tämä vaade asettaa esimerkiksi radiohiljaisuuden käytölle tai sähkömagneettisen aktiivisuuden määrälle kokonaisuutena ja jopa lähetinkohtaisesti. Yksityiskohtaiset tiettyyn tilanteeseen ja paikkaan sidotut tarkastelut edellyttävät kuitenkin sekä suojautuvan joukon, että tiedustelujärjestelmän ryhmityksen ja liikkeen mallintamista/simulointia. Laajojen tarkasteluiden tekeminen vaatisi näin ollen tätä varten valmistettuja analysointi- ja simulaattoriohjelmia.

EMCON-tasojen kriteerejä voidaan arvioida myös yksinkertaisemmin olettamalla tilanne häiriöttömäksi pois lukien radiohiljaisuudessa olevat lähettimet. Tällöin ei tarvitse tehdä mitään oletuksia tiedustelujärjestelmän käyttöperiaatteista tai suorituskyvystä eikä myöskään muista kuvautumistodennäköisyyksiin vaikuttavista seikoista. Tällainen tarkastelu on kaikkein helpoin toteuttaa. Saadut tulokset edustavat suojautujan kannalta vaikeinta mahdollista tilannetta.

5.4.2. Vertailua radioaaltojen etenemistä kuvaaviin laskentamalleihin

Elektronisen suojautumisen mahdollisuuksia voidaan arvioida erilaisten radioaaltojen etenemistä kuvaavien laskentamallien ja näitä hyödyntävien tietokoneohjelmien avulla [30, s. 101]. Tällainen mallinnus perustuu ennen muuta kentänvoimakkuuksien arviointiin eri etäisyyksillä lähettävästä laitteesta tai vaihtoehtoisesti tiedustelusensorista. Menetelmä on varsin käyttökelpoinen vaikkakin mallinnus rajoittuu arvioimaan käytännössä vain signaalin ilmaisun kriteereitä. Varsinaisesti ei siis tarkastella tiedustelijan ulottuvilla olevan informaation määrää ja sen vaikutuksia tilannekuvan tarkkuuteen. Taulukossa 5.4 on havainnollistettu yhteisinformaatioon pohjautuvan menetelmän (menetelmä 3) mahdollisuudet tuottaa lisäarvoa pelkkiin kentänvoimakkuusarvioihin verrattuna. Taulukossa esitetyt tilanteet perustuvat tässä työssä aikaisemmin esiteltyihin esimerkkeihin 4.5, 4.7, 4.8 ja 4.11.

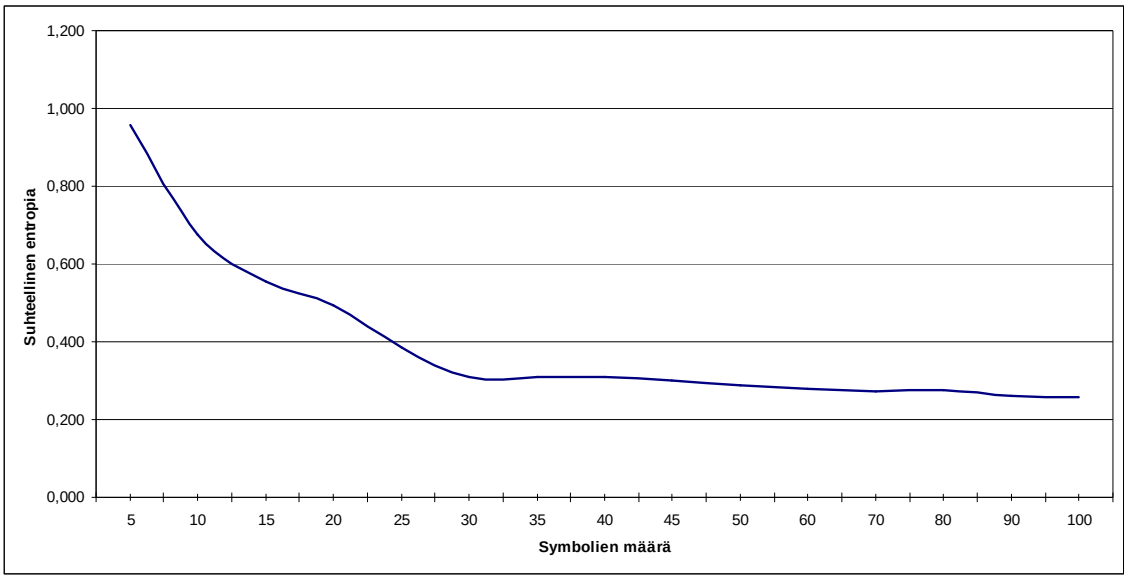
Tilanne ja kuvaus	**Ilmaistavissa olevien lähettimien määrä**	**Käytössä olevan informaation määrä.**
Tilanne 1 (ks. esimerkki 4.5). Häiriötekijät eivät vaikuta tiedustelujärjestelmän kapasiteettiin.	5	100 %
Tilanne 2 (ks. esimerkki 4.7). Havaitsemistodennäköisyyttä rajoitettu.	5	87 %
Tilanne 3 (ks. esimerkki 4.8). Yksi lähetin radiohiljaisuudessa. Havaitsemistodennäköisyyttä rajoitettu.	4	76 %
Tilanne 4 (ks. esimerkki 4.11). Havaitsemistodennäköisyyttä rajoitettu. Paikantaminen ei ole yksikäsitteistä.	5	61 %

Taulukko 5.4: Kentänvoimakkuuksien mittaamiseen ja informaatioteoreettisiin määritelmiin perustuvien arviointimenetelmien vertailua.

Taulukosta havaitaan, että jos kentänvoimakkuuteen perustuvien arviointien yhteydessä ei käytetä mitään muita analysointimenetelmiä, saadaan lopputulokseksi vain tietoisuus siitä, kuinka monta emissioympäristön lähettimistä on signaali-kohina -suhteen puolesta ilmaistavissa. Yhtenäisinformaatioon perustuva arviointimenetelmä antaa tämän lisäksi selkeän indi-

kaation siitä, kuinka paljon emissioympäristön tuottamasta informaatiosta on tiedustelijan käytettävissä. Tällöin eri tilanteiden arvottaminen on helpompaa.

Mikäli lisäksi hyödynnetään suhteelliseen entropiaan perustuvaa menetelmää 4, voidaan tehdä arvioita tilannekuvan tarkkuuden kehittymisestä tuotettujen lähetteiden funktiona. Toisin sanoen voidaan tarkastella, kuinka nopeasti tilannekuva saavuttaa suojautujan kannalta kriittisen tason. Kuvassa 5.4 on esitetty tilanteeseen 3 sidottu käyrästö, jonka perusteella tilannekuvan kehittymistä voidaan arvioida.



Kuva 5.4: Tilannekuvan tarkkuuden kehittyminen lähetteiden määrän funktiona. Kuvaaja on tuotettu simuloimalla samoin kuin luvuissa 4.4 ja 5.3 on esitetty.

On selvää, että paras arviointitulos saavutetaan, mikäli kentänvoimakkuuksien laskemiseen perustuvien menetelmien rinnalla hyödynnetään informaatioteoreettisiin menetelmiin pohjautuvia malleja.

5.4.3. Esimerkkejä hyödynnettävyydestä

Esimerkki 5.3

Testataan menetelmien 3 ja 4 avulla elektronisen aktiivisuuden vähentämisen tuottamaa lisäystä osajoukon elektronisen suojautumisen tasolle. Vertaillaan taulukossa 5.4 mainittuja tilanteita 2 ja 3, joissa erona on se, että tilanteessa 3 yksi lähetin määrätty lähetyskieltoon. Tulokset on koottu taulukkoon 5.5.

Arviointikriteeri	Tilanne 2	Tilanne 3	Viitteet
Kentänvoimakkuuden perusteella ilmaistavissa (lähetintä, kpl)	5	4	Taulukko 5.4
Tiedustelijan ulottuville päätyvä informaatio (prosenttia tuotetusta)	87	76	Esimerkit 4.7 ja 4.8. Taulukko 5.4
Saavutettu tilannekuvan tarkkuus D_{KL} = 0.3 (symbolia)	n. 22	n. 30	Kuvat 4.20 b ja 5.4.
Saavutettu tilannekuvan tarkkuus D_{KL} = 0.2 (symbolia)	n. 25	> 100	Kuvat 4.20 b ja 5.4.
Saavutettu tilannekuvan tarkkuus D_{KL} = 0.1 (symbolia)	n. 30	> 100	Kuvat 4.20 b ja 5.4.

Taulukko 5.5: Yhteenveto eri arviointimenetelmillä saatavista tuloksista. Viitteet sarakkeeseen merkitty, mihin esimerkkeihin, taulukoihin ja kuviin perustuen esitetyt lukuarvot on saatu määritettyä.

Menetelmiä 3 ja 4 hyödyntämällä saadaan selkeitä mitallisia tuloksia vertailtaessa suojautumismenetelmien tuottamaa lisäsuojaa. Tässä tapauksessa tilanteessa 3 päätyy informaatiota 11 % vähemmän tiedustelijan saataville. Tilanteessa 3 tiedustelija ei myöskään käytännössä kykene saavuttamaan alle D_{KL} = 0.2 tasoista tilannekuvaa. ◇

Esimerkki 5.4

Käsiteltävä joukko olkoon jälleen osajoukko A. Asetetaan tälle osajoukolle EMCON-tason kriteeriksi 50 % tyypillistä taistelutilannetta vastaavasta entropiasta H_{sE} = 2.13 bit/symboli. Hyödyntämällä menetelmää 3, voidaan kartoittaa, millaisilla edellytyksillä asetettu taso saavutetaan. Taulukossa 5.6 on esitetty tulokset seuraavissa olosuhteissa: a) Havaitsemistodennäköisyydet on otettu huomioon lähettimille, jotka eivät ole lähetyskiellossa. b) Tilanne oletetaan häiriöttömäksi eli havaitsemistodennäköisyyksiä ei ole huomioitu.

Radiohiljaisuudessa olevat lähettimet	a)	b)
2 kpl Lähettimet a_1 ja a_2	60.6 %	Ei laskettu
3 kpl Lähettimet a_1, a_2 ja a_3	43.2 %	68.1 %
4 kpl Lähettimet a_1, a_2, a_3 ja a_4	Ei laskettu	46.5 %

Taulukko 5.6: Olosuhteiden vaikutus tiedustelujärjestelmän suhteelliseen kapasiteettiin.

Todetaan, että mikäli häiriöiden vaikutus kyetään ottamaan huomioon tarkastelussa, tulee vähintään kolmen lähettimen olla radiohiljaisuudessa, jotta asetettu EMCON-kriteeri täytetään. ”Varman päälle” laaditussa arviossa tilanne oletetaan häiriöttömäksi ja tällöin neljän lähettimen on oltava radiohiljaisuudessa. Näiden tulosten perusteella lähetin a_5 saisi liikennöidä vapaasti, mutta muilta liikennöinti olisi kielletty. On huomattava, että esimerkissä ei ole etsitty

muita vaihtoehtoisia keinoja saavuttaa asetettu EMCON-kriteeri. Lukijan on syytä myös perehtyä luvussa 5.4.4 esitettyyn jatkopohdintaan tämän esimerkin tulosten osalta. ◇

Esimerkki 5.5

Lähteessä [38, s. 130] on esitetty, että eräs ad hoc –verkkojen elektronisen suojautumisen keino on viestiliikenteen jakaminen tasaisesti verkon eri reiteille, jolloin ei muodostu aktiivisuudeltaan muista erottuvia solmuja. Tässä esimerkissä osoitetaan, että kehitetyt menetelmät tarjoavat keinon mitallisesti arvioida, kuinka paljon tällainen suojautumiskeino parantaa verkon elektronisen suojautumisen tasoa.

Helpoin tapa toteuttaa arvio, on mieltää emissiomallin tuottama entropian määrä siten, että se on epävarmuus, joka vallitsee ennen jonkin todennäköisyyksiin perustuvan kokeilun toteuttamista (ks. [55]). Elektronisen suojautumisen kannalta on siis parasta tuottaa mahdollisimman paljon epävarmuutta sähkömagneettiseen spektriin. Tämä toteutuu liikenteen ollessa mahdollisimman tasajakautunutta eri solmupisteissä. On huomattava, että elektronisen suojautumisen tason kannalta tällä arviointitavalla ei voida vertailla keskenään tilanteita, joissa emissioympäristössä olevien lähettimien (symboleiden) määrä vaihtelee. Oletetaan, että lähtökohtaisesti verkko noudattelee osajoukon A määrittelyjä (ks. esimerkki 4.5). Esimerkissä 4.5 on laskettu tarvittavat entropiat: $H_s = 2.13 \frac{bit}{symb}$ ja $H_{sU} = 2.32 \frac{bit}{symb}$. Tasaisesti jaettu liikenne tarjoaa näin ollen noin 9 % paremman elektronisen suojautumisen tason, kuin alkuperäinen tilanne (H_s). Ero ei ole kovin suuri, koska osajoukon A ominaisuudet ovat jo alun perin varsin tasajakautuneet. Vastaava suojautumisen tason parantuminen osajoukolle D (ks. esimerkki 4.5) olisi noin 48 %.

Epävarmuus jonkin kokeilun lopputuloksesta ennen kokeen suorittamista on sama, kuin informaation määrä, joka odotetaan saatavan käyttöön kokeen toteuttamisen jälkeen [1, s. 29]. Tähän tulkintaan perustuen voidaan ajatella, että tiedustelujärjestelmä pyrkii saamaan käyttöönsä mahdollisimman paljon tuotetusta informaatiosta. Menetelmällä 3 voidaan arvioida tuota informaation määrää kuitenkin muistaen, että tässä tapauksessa vertaillaan olosuhteita, joissa esiintymistodennäköisyysjakaumat ovat erilaiset. Tällöin suhteellinen vertailu ei yksistään riitä, vaan on myös vertailtava ehdollisia entropioita (ks. luku 4.3.4). Osajoukolle A voidaan laskea tiedustelujärjestelmän normalisoidut kapasiteetit sekä alkuperäiseen tilanteeseen sitoen, että tasajakaumaan sitoen. Lähtökohtatilanne oletetaan esimerkin 4.7 mukaiseksi. Tällöin saadaan arvoiksi $D_N^s = 0.869$ ja $D_N^{sU} = 0.872$. Nähdään, että tasajakauman kyseessä ollessa normalisoitu kapasiteetti on itse asiassa suurempi, kuin alkuperäisessä tilanteessa. Tämä

johtuu esiintymistodennäköisyyksien ja kuvautumistodennäköisyksien kombinaatioista, jotka tässä tilanteessa toimivat siten, että tasajakautuneessa tilanteessa informaatiota päätyy suhteellisesti enemmän tiedustelujärjestelmän saataville. Tilanteen arvioimiseksi on laskettava myös ehdolliset entropiat yhtälön 4.40 avulla. Nyt saadaan $H^{s}(\cdot\,|\,\cdot) = 0.2789 \frac{bit}{symboli}$ ja $H^{sU}(\cdot\,|\,\cdot) = 0.2979 \frac{bit}{symboli}$, eli $H^{sU}(\cdot\,|\,\cdot) > H^{s}(\cdot\,|\,\cdot)$. Voidaan siis todeta, että esiintymistodennäköisyysjakauman ollessa tasajakauma saavutetaan tässä tilanteessa absoluuttisesti noin 0.02 bit/symb etu verrattuna alkuperäiseen tilanteeseen. Prosenttiyksiköinä ilmaistuna tilanne paranee noin 6.8 %. Elektronisen suojautumisen tason kannalta tasajakauma on siis hieman parempi, kuin lähtökohtajakauma.

On huomattava, että joissain tilanteissa on mahdollista päätyä tulokseen, jossa tasajakaumalla ei saavuteta etua muihin jakaumiin nähden. Tämä johtuu verrokkitilanteen esiintymistodennäköisyyksien määrittelyistä ja siitä, miten kuvautumistodennäköisyydet niitä kohtelevat kanavalla. Menetelmän 3 avulla saatava tulokset ovat mitä suurimmassa määrin tilannesidonnaisia.

Tasajakauma on kuitenkin elektronisen suojautumisen kannalta aina tavoittelemisen arvoinen tilanne, koska se tuottaa aina suurimman ehdollisen entropian, mikäli tiedustelujärjestelmän normalisoitu kapasiteetti on tarkasteltavien tilanteiden kesken sama. Tämä osoitettiin luvussa 4.3.4. ◇

5.4.4. Menetelmien käytettävyyden kannalta huomioitavia ja rajoittavia tekijöitä

Esiteltyjen informaatioteoriaan pohjautuvien menetelmien käytettävyys edellyttää muutamien perusolettamusten voimassaoloa ja hyväksymistä. Useita yksityiskohtia, jotka kuitenkin ovat tärkeitä menetelmien käytännöllisen soveltamisen kannalta, on tässä työssä jätetty vain teoreettiselle tai kevyelle tarkastelulle. Seuraavassa on kartoitettu näitä menetelmien käytettävyyden kannalta huomioitavia ja mahdollisesti myös rajoittavia tekijöitä. Luvussa on myös lyhyesti hahmoteltu millaisilla edellytyksillä esitellyt menetelmät olisivat käyttökelpoisia käytännön työkaluja.

Menetelmien käytettävyys edellyttää, seuraavien perusolettamusten voimassaoloa ja hyväksymistä.

1) Joukkojen ja osajoukkojen sisältämää sekä tuottamaa informaatiota voidaan kuvata ja analysoida tilastollisiin todennäköisyysjakaumiin perustuen. Tässä työssä käytetty informaation määrän määrittely on yleisesti hyväksytty ja käytetty, joten lähtökohta tälle

olettamukselle on vahva. Osaltaan tässä työssä esitetyt tarkastelut myös todistavat, että käyttökelpoisia tuloksia saadaan tuotettua tämän olettamuksen varaan.

2) Informaation semantiikkaa ei huomioida arvotettaessa informaation määrää. Näin ollen esimerkiksi viestiliikenteen sisällöllä ei oleteta tuotettavan lisäarvoa tiedustelijalle. On kuitenkin huomattava, että myös lähetteiden ulkoisten ominaisuuksien voidaan katsoa tuottavan semantiikan piiriin kuuluvaa tietoa. Ulkoisten parametrien perusteella luokitellaan/tunnistetaan lähete tietynlaiseksi (ks. luku 2.2.2). Etenkin menetelmien 1 ja 2 käytettävyyden osalta perusolettamuksena on, että tiedustelija kykenee erottamaan erilaiset lähetteet toisistaan ulkoisten parametrien perusteella. Tällä oletuksella on vaikutuksia myös hyödyntämistodennäköisyyksien määräytymiseen ja tätä kautta edelleen menetelmien 3 ja 4 käytettävyyteen.
3) Osajoukkojen ja joukon sähkömagneettinen aktiivisuus voidaan kuvata riittävän luotettavalla emissiomallilla ja emissiomalli kyetään laatimaan Markov prosessin ominaisuuksien mukaisesti. Yksityiskohtainen osajoukon emissiomallin laatiminen edellyttää osajoukon sähkömagneettisen käyttäytymisen tarkkaa analysointia. Todennäköisesti on kuitenkin niin, että melko karkeallakin mallinnuksella voidaan vertailla erilaisten olosuhteiden vaikutusta osajoukon ja joukon elektroniseen aktiivisuuteen sekä elektronisen suojautumisen tasoon. Mallintamismahdollisuuksien selvittäminen todellisten joukkojen ja organisaatioiden osalta sekä mahdollinen mallintaminen vaativat jatkotutkimusta.
4) Joukko kyetään jakamaan käytännöllisiin ja toisistaan suhteellisen riippumattomiin osajoukkoihin. Osajoukkojen rakenteelle ei ole annettu mitään tiukkaa mallia, vaan ne on muodostettava parhaiten tilanteeseen sopivalla tavalla (ks. luvut 4.2.2, 4.2.4 ja 4.3.1). Emissiomalleja varten muodostettuja osajoukkoja ei tarvitse rakentaa siten, että niissä on edustettuna vain yksi lähetetyyppi. Osajoukkojen riippumattomuus (kukin lähetinyksilö kuuluu vain yhteen osajoukkoon) korostuu etenkin menetelmiä 3 ja 4 käytettäessä. Luvussa 5.2.1 on toki esitetty tapa, jolla yksi lähetinyksilö voidaan jakaa kuuluvaksi useaan eri osajoukkoon. Tarkasteluista tulee tällöin kuitenkin monimutkaisempia ja tätä on pyrittävä välttämään.
5) Kuvautumistodennäköisyydet kyetään mallintamaan riittävällä tarkkuudella. Kuvautumistodennäköisyydet näyttelevät merkittävää roolia yhtenäisinformaatioon ja suhteelliseen entropiaan perustuvissa tarkasteluissa. Luvussa 4.3.3 on esitelty, miten sieppaus-, ilmaisu- ja hyödyntämistodennäköisyydet voidaan huomioida kuvautumistodennäköisyyksien määrittämisessä. Voidaan arvioida, että ilmaisu- ja hyödyntämistodennäköisyyksien huomioiminen on esiteltyjen rajausten ja määritelmien puitteissa

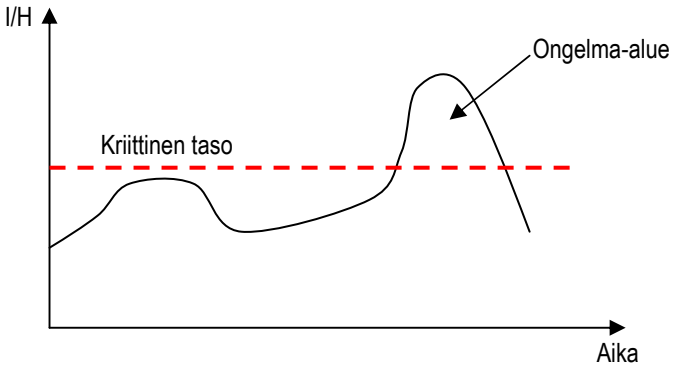
mahdollista etenkin, jos tarkastelujen tukena käytetään radioaaltojen etenemistä simuloivia tietokoneohjelmistoja. On toki huomattava, että maastoon sidotut tarkastelut edellyttävät joukon ryhmityksen ja liikkeen sekä tiedustelujärjestelmän sijainnin simuloimista[14]. Sieppaustodennäköisyyksien osalta todettiin, että yksityiskohtiin menevien laskelmien sijasta priorisoidaan emissioympäristön kohteet ja oletetaan, että tiedustelija käyttää resurssejaan eniten tärkeimpien kohteiden sieppaamiseen. Tällöin näiden kohteiden sieppaustodennäköisyydet ovat suurimpia. Tällainen parametrointi edellyttää jatkoselvityksiä, joissa arvioidaan organisaatio- ja taistelutilannekohtaisesti tiedustelijan kannalta mielenkiintoisimmat kohteet.

6) Joukkokokonaisuuksien tuottama entropia ja tiedustelujärjestelmän ulottuville päätyvä informaatio voidaan määrittää informaation yhteenlaskettavuutta hyödyntäen. Tällöin osajoukkojen (vast.) tulee olla toisistaan riippumattomia kokonaisuuksia.

Menetelmä 1 on helpoiten suoraan hyödynnettävissä, koska siihen pohjautuvat analyysit voidaan toteuttaa perustuen joukko- ja kalustoluetteloihin eikä erillistä mallien rakentamista sinänsä tarvita. Työkaluksi soveltuu taulukkolaskentaohjelma.

Menetelmien 2 ja 3 avulla voidaan laatia yksittäiseen ajanhetkeen ja lähetinmäärältään rajoittuneita tarkasteluja manuaalisesti. Tällaisia ovat myös tässä työssä esitetyt esimerkit 4.2, 4.3, 4.5, 4.7, 4.8 ja 4.11. Mikäli halutaan analysoida monimutkaisia tilanteita jonkin tietyn aikaikkunan puitteissa, tulee kyetä mallintamaan joukon / osajoukon liike ja erilaisten häiriöitä aiheuttavien tekijöiden vaikutus tilanteeseen (esim. maaston vaikutus). Tällaiset tarkastelut eivät käytännössä ole mahdollisia ilman tätä varten valmistettuja analysointi- ja simulointiohjelmistoja. Aikaan ja paikkaan sidotut tulokset voisivat antaa hedelmällisiä tuloksia, koska tällöin mahdolliset ongelma-alueet kyettäisiin havaitsemaan. Kuvassa 5.5 on hahmotelma tällaisen tarkastelun mahdollisesti tuottamista tuloksista.

[14] Taistelun simulointiin liittyvää kirjallisuutta on olemassa runsaasti. Aiheeseen liittyvään problematiikkaan ja Suomessa lähiaikoina tehtyihin tutkimuksiin voi perehtyä esimerkiksi teoksen [27] kautta.



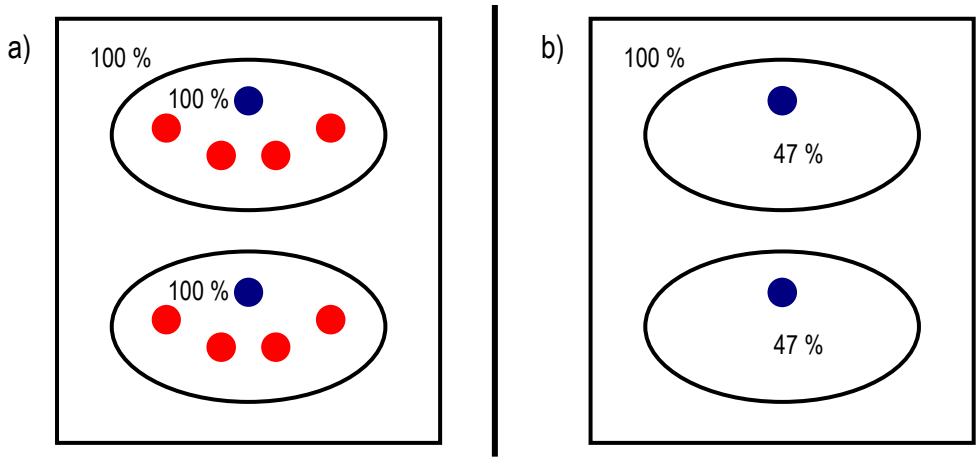
Kuva 5.5: Mikäli tiedustelijan ulottuville päätyvä informaation suhteellinen määrä (I/H) voidaan esittää ajan funktiona, on mahdollista löytää ajankohdat ja alueet, jolloin joukko tai osajoukko on erityisen haavoittuva tiedustelulle.

Menetelmän 4 avulla voidaan laatia yksinkertaisia arvioita esimerkiksi simuloimalla emissioympäristöä satunnaisluvuilla taulukkolaskentaohjelmassa (ks. liite 7). Tämän työn esimerkit 4.12, 4.13 ja 5.2 on toteutettu näin. Laajat kokonaisuudet voivat kuitenkin olla melko työläitä pelkästään taulukkolaskentaohjelman varassa toteutettuina. Lisäksi on huomattava, että tämän työn esimerkit on laadittu staattisessa tilanteessa, jossa lähetteiden kuvautumisissa ei tapahdu muutoksia tarkastelujakson aikana. Tällaiset tarkastelut toki ovat varsin riittäviä, jos halutaan tutkia erilaisten emissiomalliin tehtävien muutosten vaikutusta suhteelliseen entropiaan eli tilannekuvan laatuun. Tiettyyn tapahtumaan (esim. operaatioon) sidotut tarkastelut edellyttävät tämänkin menetelmän kohdalla joukkojen liikkeen ja häiriötekijöiden tarkempaa mallintamista erillisiä analysointiohjelmistoja käyttäen.

Emissiomalli luo pohjan menetelmien 3 ja 4 käytölle. Arvioitaessa radiohiljaisuuden tai lähetyskieltojen vaikutuksia osajoukon tai joukon elektronisen suojautumisen tasoon, saadaan selkeitä mitallisia tuloksia erilaisten olosuhteiden välille. Tässä työssä ei kuitenkaan ole tarkasteltu sitä, vaikuttaako joidenkin lähettimien asettaminen radiohiljaisuuteen muiden samassa emissiomallissa olevien lähettimien käyttäytymiseen. Oletuksena on siis ollut, että emissiomallin mallinnus säilyy samanlaisena, vaikka osa lähettimistä on ei-aktiivisia. Tutkittua tietoa tämän tyyppisistä seikoista ei ole ollut saatavilla, joten asiaan ei ole otettu tarkemmin kantaa. Mikäli aktiivisten asemien käyttäytyminen muuttuisi huomattavasti alkuperäiseen malliin nähden, lienee mahdollista rakentaa uusi emissiomalli kuvaamaan tätä tilannetta. Ei-aktiivisten lähettimien sisällyttäminen tähän uuteen malliin voi kuitenkin olla varsin haastavaa.

Kehitettyjä menetelmiä hyödynnettäessä on huomioitava, että kukin menetelmä tarkastelee elektronista aktiivisuutta ja elektronisen suojautumisen tasoa tietystä näkökulmasta ja tietystä

kohtaa mallia, jolla kuvataan tilannekuvan muodostumista (ks. luku 4.1.1). Kuten todettua, menetelmät perustuvat tilastollisten todennäköisyysjakaumien käsittelyyn informaatioteoreettisista lähtökohdista. Mallinnuksessa ei siis oteta huomioon tiedustelujärjestelmässä työskentelevän ihmisen tai tietojärjestelmän mahdollisesti muista näkökulmista tehtyjä johtopäätöksiä. Tämä rajoite on huomioitava tarkasteltaessa joitain menetelmillä aikaansaatuja tuloksia. Esimerkkinä toimii luvussa 5.4.3 esitelty esimerkki 5.4, jossa ns. ”varman päälle” laskettu 50 % EMCON-kriteeri edellyttää, että viidestä lähettimestä vain johtoasema saa liikennöidä ja ala-asemat ovat radiohiljaisuudessa. Tällöin tuotetun entropian määrä on 46.5 % tyypillistä taistelutilannetta vastaavasta entropiasta. Onko tiedustelujärjestelmän mahdollista tuottaa näin ollen vain noin 47 %:esti oikea tilannekuva? Vastaus on kyllä, mikäli tiedustelujärjestelmä on nimenomaan kiinnostunut johtoaseman alaisuudessa toimivista alijoukoista ja tilannekuva rakennetaan perustuen myös tämän alimman tason ”informaatiovarantoon”. Toisaalta tiedustelujärjestelmällä on mahdollisuus rakentaa 100 % oikea tilannekuva, jos ollaan kiinnostuneita joukosta kokonaisuutena. Tällöin pelkkä johtoaseman löytyminen voi riittää tiedustelijalle halutun tilannekuvan tuottamiseksi. Tämä edellyttää, että tiedustelujärjestelmä kykenee tekemään johtopäätöksiä vajavaisen informaation pohjalta. Tällöin ei kuitenkaan enää puhtaasti pidättäydytä tilastollisessa informaationäkökulmassa, joka on tämän työn perusolettamus. Tässä kerrotun opetus on se, että esitellyt menetelmät eivät varsinaisesti kuvaa tiedustelujärjestelmän toimintaa, vaan ainoastaan sen vastaanottaman informaation määrää. Tämä on huomioitava, mikäli menetelmien avulla saatuja tuloksia sovelletaan käytäntöön. Kuvassa 5.6 on havainnollistettu yllä esitettyä problematiikkaa.



Kuva 5.6: a) Kaksi osajoukkoa, joiden kaikki lähettimet käytettävissä tilannekuvan muodostamiseksi. 100 % informaatiosta käytettävissä tilannekuvan muodostamiseen koko joukosta. b) Osajoukoista vain johtoasemat käytettävissä tilannekuvan muodostamiseen eli informaatiosta n. 47 %. Informaation yhteenlaskettavuuden mukaisesti tällöin olisi käytössä 47 % myös koko joukon entropiasta. Tiedustelija voi kuitenkin johtopäätöksiin perustuen kyetä rakentamaan tilannekuvan, jossa osajoukkojen olemassa ololle riittävän varmuuden antaa johtoasemien havainnointi eikä ala-asemista olla kiinnostuneita. Tästä näkökulmasta katsoen tiedustelijalla on 100 % tilannekuva.

6. TULOKSET JA JOHTOPÄÄTÖKSET

6.1. Tutkimustulokset

6.1.1. Kehitetyt menetelmät

Tämän tutkimuksen päätehtävänä on ollut löytää, informaatioteoreettiseen näkökulmaan sitoen, menetelmiä joukon ja sen osajoukkojen sisältämän sekä tuottaman informaation arvioimiseksi siten, että näitä menetelmiä voidaan hyödyntää elektronisen aktiivisuuden ja elektronisen suojautumisen arvioinnissa. Tuotetun informaation osalta tavoitteena on ollut myös luoda menetelmä (emissomalli), jolla voidaan kuvata osajoukkojen aktiivisuuta sähkömagneettisen spektrin osalta. Tässä luvussa esitellään tiivistäen luvuissa 4 ja 5 johdetut menetelmät ja se, millaisia tuloksia löydetyillä menetelmillä on mahdollisuus tuottaa.

Menetelmä 1: Joukon lähetejakauman analysointi (luku 4.2.2).
Menetelmä perustuu organisaation eri tasoille sijoitetun lähetinkaluston jakautumisen analysointiin entropian avulla. Menetelmän avulla kyetään havaitsemaan organisaatiosta ne osajoukot, jotka ovat lähetejakaumansa puolesta kaikkein heterogeenisimpiä suhteessa koko joukkoon. Toisin sanoen tiedustelija kykenee erottamaan nämä osajoukot kaikkein helpoiten sähkömagneettiseen sormenjälkeen perustuen. Monissa tapauksissa tämä ominaisuus on toki pääteltävissä ilman erillisiä analyysejakin, mutta esiteltyä menetelmää voidaan puolustaa sillä, että se antaa mahdollisuuden yksiselitteiseen, mitalliseen ja konkreettiseen eri osajoukkojen ja joukkojen vertailuun. Mitallisuus tarkoittaa, että voidaan vertailla keskenään kuinka paljon huomaamattomampi jokin osajoukko on suhteessa toiseen.

Menetelmä 2: Kriittisen toiminnan tunnistaminen (luku 4.2.3).
Yhtenäisinformaation hyödyntämiseen perustuva menetelmä arvioi, kuinka helposti jokin kriittinen toiminta on eroteltavissa ympäristöstään. Käytännössä johonkin toimintaan liittyvän osajoukon tai osajoukkojen lähettimet on sijoitettu maantieteelliselle alueelle, jossa saattaa toimia muitakin osajoukkoja. Menetelmällä pyritään selvittämään, miten helposti mielenkiinnon kohteena oleva toiminta on tunnistettavissa lähetejakaumiin perustuen, kun samalla alueella toimivat muut joukot mahdollisesti vaikeuttavat tiedustelijan toimintaa. Se, miten tarkasteltava kriittinen toiminta määritellään, on oleellista tarkastelun kannalta. Tarkastelu korostaa helposti luokiteltavien ja yksilöitävien lähetteiden osuutta tiedustelijan epävarmuuden vähen-

täjinä. Matemaattisesti menetelmä perustuu rajoitukseen, jossa vain saman maantieteellisen solun sisällä olevat identtiset lähetteet voivat vaikeuttaa tiedustelijan tilannekuvan muodostamista. Solujen koon valintaa on käsitelty melko karkeasti, joten lisätarkastelut tämän suhteen voisivat olla paikallaan. Käytännössä solun koossa tulee huomioida ainakin lähettimien pienimuotoinen (hyvin rajatulla alueella tapahtuva) liike taistelukentällä, joka saattaa vaikeuttaa erottelua muista samalla alueella toimivista ja identtisistä lähetteistä. Tämän menetelmän avulla voidaan kuvata vaikeusaste, jolla jokin toiminta on hahmotettavissa tietyltä maantieteelliseltä alueelta lähetekategorioihin (ks. luku 4.2.2) perustuen.

Menetelmä 3: Tiedustelujärjestelmän ulottuville päätyvän informaation määrän arviointi (luvut 4.3 ja 5.2)

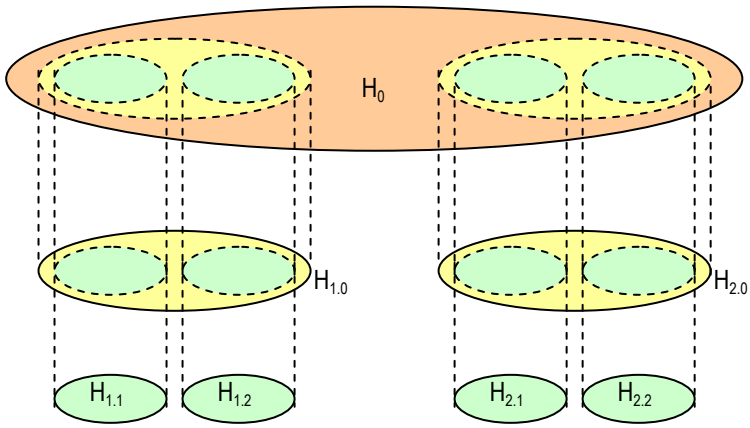
Menetelmän perusidea on tiedustelujärjestelmän suhteellisen kapasiteetin mieltäminen yhtenäisinformaatioksi tiedustelujärjestelmän vastaanottaman informaation ja emissioympäristön tuottaman informaation välillä. Voidaan siis arvioida, kuinka paljon informaatiota tiedustelija kykenee saamaan käyttöönsä, kun joukko tai osajoukko käyttää lähettimiään jollain määrätyllä tavalla. Periaatteessa on mahdollista tarkastella yksittäisen lähettimen tarkkuudella, kuinka paljon informaatiota päätyy tiedustelijan ulottuville tilanteissa, joissa ko. lähettimen käyttöä ei ole rajoitettu verrattuna tilanteisiin, joissa rajoituksia on olemassa. Erilaisten olosuhteiden vertailu edellyttää emissiomallin ja kuvautumistodennäköisyyksien säätämistä. Mikäli halutaan vertailla olosuhteita tai osajoukkoja, joiden emissiomallit (esiintymistodennäköisyydet ja symbolinopeudet) poikkeavat toisistaan, on yhtenäisinformaatioon perustuvan tarkastelun rinnalle nostettava ehdolliseen entropiaan perustuva analyysi. Ehdollisen entropian avulla voidaan arvioida, kuinka paljon tuotetusta informaatiosta jää absoluuttisesti tiedustelujärjestelmän ulottumattomiin. Tällöin kaikkien mahdollisten olosuhteiden vertailu mitallisesti on mahdollista.

Menetelmä 4: Tilannekuvan tarkkuuden arviointi suhteellisen entropian avulla (luvut 4.4 ja 5.3).

Menetelmä perustuu oletukseen, jossa tiedustelujärjestelmän muodostaman tilannekuvan ja todellisen emissioympäristön välistä epäsovitusta voidaan mitata suhteellisen entropian avulla. Menetelmä pohjaa rakenneanalyysiin, jossa tiedustelijan tavoitteena on luoda kuva vastustajan elektronisesta taistelujaotuksesta perustuen mm. radioverkkojen rakenteen selvittämiseen [22, s. 135 - 138] ja [39, s. 174]. Rakenteen selvittäminen saattaa usein vaatia ainakin jonkinasteista havaittujen lähetteiden tilastollista käsittelyä, jotta eri kohteiden erot elektronisen aktiivisuuden osalta paljastuvat. Tilastollinen tiedonkäsittely on myös oleellinen osa pro-

sessointia, jolla tilannekuva muodostetaan sensori- ja datafuusiota hyödyntävissä automaattisissa tilannekuvajärjestelmissä [24]. Tietämystä emissiomallin tilastollisesta rakenteesta voidaan näiden näkökulmien valossa pitää varsin hyvänä tilannekuvan laadun mittarina. Suhteellinen entropia on sopiva työkalu käytettäväksi tämän tyyppisiin tarkasteluihin. Menetelmä kuitenkin korostaa emissiomallin ja ns. vakaan todennäköisyysjakauman oikeellisuuden merkitystä ainakin, jos halutaan kartoittaa havaintomääriä (symbolien määriä), joita tarvitaan tilastollisesti laadukkaan tilannekuvan tuottamiseen. Menetelmä soveltuu hyvin erilaisten olosuhteiden ja elektronisten suojautumismenetelmien vaikutusten vertailuun tilannekuvan laadun suhteen. Erilaisten olosuhteiden vertailu edellyttää emissiomallin ja kuvautumistodennäköisyyksien säätämistä.

Työn painopiste on ollut esiteltyjen menetelmien laatiminen osajoukkojen elektronisen aktiivisuuden ja elektronisen suojautumisen arviointiin. Etenkin menetelmät 1 ja 2 vaativat aina viitekehyksekseen jonkin kokonaisen joukon, jonka suhteen lähetetodennäköisyydet ovat määriteltävissä. Menetelmien 3 ja 4 soveltaminen monta osajoukkoa sisältävään joukkoon perustuu informaation yhteenlaskettavuuteen. Tämä on varsin suoraviivainen ja helppo keino toteuttaa suurienkin kokonaisuuksien tarkastelut. Yhteenlaskettavuus kuitenkin edellyttää, että tarkastelussa käytetyn alimman tason muodostavat osajoukot ovat toisistaan riippumattomia, eli yksittäinen lähetin voi sisältyä vain yhteen alimman tason osajoukkoon. Riippumattomuuden tulee säilyä kaikilla organisaation tasoilla. Luvussa 5.2.1 on esitelty menetelmä, jolla yksittäinen lähete voidaan tarvittaessa sisällyttää useaan eri osajoukkoon, mutta tällöinkin osajoukkojen riippumattomuuden tulee säilyä. Kuvassa 6.1 on havainnollistettu informaation yhteenlaskettavuutta ja osajoukkojen riippumattomuutta.



Kuva 6.1: Joukon entropian muodostuminen osajoukkojen summana.
Kuvassa $H_0 = H_{1.0} + H_{2.0} = H_{1.1} + H_{1.2} + H_{2.1} + H_{2.2}$.

Emissiomallilla on oleellinen rooli menetelmien 3 ja 4 kohdalla. Emissiomallin lähtökohdaksi otettiin suoraan Shannonin määritelmä [62, s. 4 - 10] diskreetille informaation lähteelle, jonka tilastollista käyttäytymistä ohjaa Markov ketju. Alkuperäistä ajatusta on sovellettu siten, että informaation lähteen katsotaan tuottavan symboleita, jotka kuvaavat lähettimien sähkömagneettiseen spektriin tuottamia lähetteitä (signaaleja). Emissiomalli kuvaa elektronista aktiivisuutta sähkömagneettisen spektrin osalta. Se ei kuvaa esimerkiksi sitä, kelle tuotettu viestiliikenne on suunnattu.

Luvussa 4.3.3 esiteltiin, miten kaikki tiedustelujärjestelmän suhteellista kapasiteettia vähentävät häiriöt voidaan huomioida kuvautumistodennäköisyyksissä. Kuvautumistodennäköisyyksissä huomioidaan näin ollen kaikki lähetteiden sieppaamiseen, ilmaisuun ja hyödyntämiseen liittyvät häiriötekijät. Kuvautumistodennäköisyydet ovat erityisen tärkeitä menetelmien 3 ja 4 kannalta. Myös menetelmä 2 hyödyntää kuvautumistodennäköisyyksiä, mutta tämän menetelmän kohdalla kuvautumista määrittää vain samassa solussa sijaitsevien identtisten lähettimien lukumäärä.

Menetelmien kehittämisen sivutuotteena on syntynyt melkoinen joukko uusia käsitteitä, määritelmiä sekä muutama matemaattinen lause todistuksineen. Näitä voidaan myös pitää tutkimustuloksina, vaikkakaan niiden kehittäminen ei ole ollut itsetarkoitus. Käytettyjä todennäköisyyskäsitteitä on esitelty luvussa 4.1.2. Muita keskeisiä määritelmiä ovat mm. joukon sisäinen ja ulkoinen informaatio (luku 1.2), lähetekategoria (luku 4.2.2), tiedustelujärjestelmän suhteellinen kapasiteetti, tiedustelujärjestelmän normalisoitu kapasiteetti sekä absoluuttinen kapasiteetti (luku 4.3.4). Työn kannalta tarpeelliset matemaattiset lauseet ja niiden todistukset on sisällytetty liitteisiin 1, 4 ja 5.

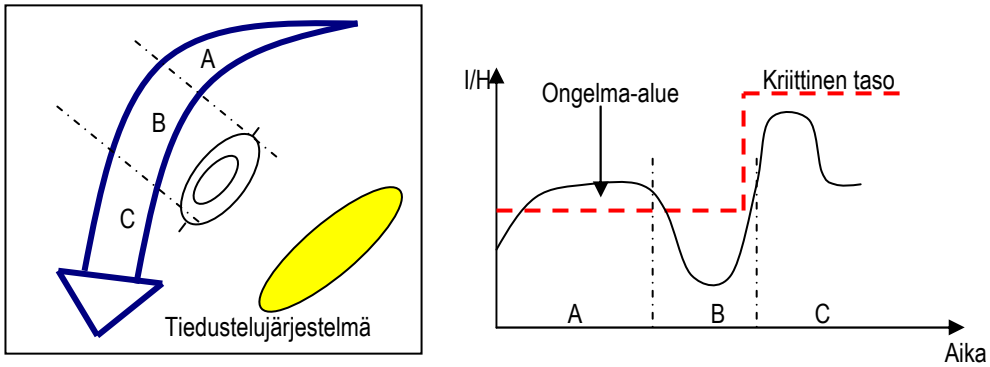
6.1.2. Menetelmien hyödyntäminen

Menetelmien 1 ja 2 hyödyntämiskohteina ovat erityisesti analyysit, joissa kartoitetaan jonkin organisaation osajoukkojen keskinäistä erottuvuutta tai koko joukon erottuvuutta toimintaympäristöstään. Menetelmää 2 voidaan hyödyntää myös arvioitaessa omia taktisia toimintavaihtoehtoja ottaen kuitenkin huomioon, että menetelmä ei mallinna sitä, miten erilaisia lähettimiä käytetään. Menetelmä 2 perustuu puhtaasti organisaation lähetejakaumaan pohjautuvaan analysointiin.

Menetelmiä 3 ja 4 voidaan erityisesti hyödyntää vertailtaessa erilaisten toiminnallisten emissioiden hallintatoimenpiteiden (EMCON) vaikutuksia joukon elektronisen aktiivisuuden ja elektronisen suojautumisen tasoon. Taktisten toimenpiteiden vertailu on myös mahdollista liittyen joukon taktisten toimintavaihtoehtojen tarkasteluun, esim. liikkeen suuntaamiseen. Tekniset suojautumisen menetelmät vaikuttavat tyypillisesti signaalien sieppaamiseen ja ilmaisuun. Tällaisten suojautumiskeinojen arviointi onnistuu, mikäli teknisten menetelmien vaikutukset kuvautusmistodennäköisyyksiin on riittävällä tarkkuudella määriteltävissä.

Lisäarvoa erilaisille tarkasteluille esitellyt menetelmät tuovat erityisesti konkreettisten ja mitallisten tulostensa osalta. Vertailujen tulokset voidaan aina esittää informaation määrää kuvaavina lukuarvoina, suhteellisina osuuksina tai esimerkiksi kuvaajina. Tällöin on mahdollista arvottaa erilaisia toimintavaihtoehtoja ja elektronisen suojautumisen toimenpiteitä perustellusti.

Kaikkia menetelmiä voidaan hyödyntää rajoitetusti manuaalisin menetelmin. Suurien joukkokokonaisuuksien yksityiskohtainen tarkastelu kuitenkin edellyttäisi tietokoneavusteista mallinnusta ja simulointia, joissa tulisi kyetä ottamaan huomioon joukkojen ryhmitys, liike ja erilaisten häiriötekijöiden vaikutus. Tämä pätee erityisesti menetelmiin 2, 3 ja 4. Menetelmä 1 ei vaadi erillisiä mallinnus- tai simulointiohjelmaa. Erityisesti menetelmien 2 ja 3 kohdalla kunnolliset mallinnusmahdollisuudet voisivat tuottaa käyttökelpoisia tuloksia, joissa yhden ajanhetken sijaan kyetään analysoimaan esimerkiksi koko operaation kesto elektronisen aktiivisuuden ja elektronisen suojautumisen näkökulmasta. Kuvassa 6.2 on esimerkki tällaisen analyysin mahdollisesti tuottamasta hyödystä. On huomattava, että tämän kaltaisten tulosten tuottamista ei ole tässä työssä käytännössä todennettu, joten mahdolliset lisätutkimukset tämän suhteen ovat paikallaan.

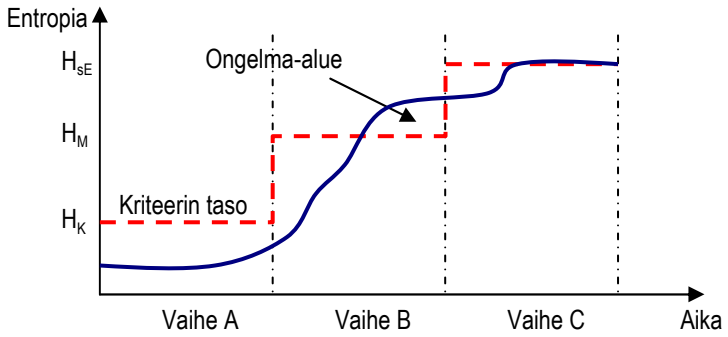


Kuva 6.2: Tiedustelujärjestelmän ulottuvilla vaiheissa A, B ja C oleva informaatio ajan funktiona. Joukon elektroninen aktiivisuus on vaiheessa A liian suuri asetettuun kriteeriin nähden. Aktiivisuutta on vähennettävä esim. tiukemmilla EMCON toimenpiteillä. Vaiheessa B elektronisen aktiivisuuden taso alittaa asetetun kriteerin. Vaiheessa C kriteeriä on nostettu.

Menetelmä 4 soveltuu sellaisenaan hyödynnettäväksi erilaisten emissiomalleihin tehtyjen muutosten vaikutusten arviointiin. Laajoja kokonaisuuksia käsittävä dynaaminen analyysi edellyttää automatisoitua työkalua.

Emissioiden hallinnan osalta on mahdollista luoda ns. EMCON-kriteeristö kokonaan uudenlaisesta näkökulmasta, joka perustuu ennen muuta arvioon siitä, kuinka paljon joukon tuottamasta informaatiosta on tiedustelijan saatavilla. Tarkimmat tulokset saadaan mallintamalla suojautuvan joukon ja tiedustelujärjestelmän käyttäytyminen sekä tilanteeseen vaikuttava häiriöt. Tiedustelijan käsiin joutuvalle informaatiolle voidaan asettaa kriteerit, joiden alle joukon tulee päästä. Tilanne vastaa kuvassa 6.2 esitettyä.

Yleisempi keino on asettaa EMCON-kriteerit suhteessa tyypillistä taistelutilannetta vastaavaan entropiaan H_{sE}. Nyt tiedustelijan ulottuville päätyvän informaation on pysyttävä kullekin operaation vaiheelle asetettujen EMCON-kriteerien alapuolella. Laatimalla emissiomallit riittävän tarkasti, voidaan menetelmällä 3 testata, millä tavalla elektronista aktiivisuutta on säädeltävä, jotta kriteerien alapuolelle päästään. Menetelmää 3 voidaan soveltaa siten, että tilanne oletetaan muuten häiriöttömäksi, mutta mahdollisesti radiohiljaisuudessa olevat lähettimet tuottava ”välilyöntejä”. Analyysien perusteella tehdyt johtopäätökset voidaan liittää EMCON ohjeistukseen. Kuvassa 6.3 on havainnollistettu tätä EMCON-kriteerien määrittämistapaa.



Kuva 6.3: Eri ajallisille vaiheille asetettu EMCON-kriteerit H_K, H_M ja H_{sE}, joiden alle menetelmällä 3 lasketun yhtenäisinformaation on jäätävä (sininen käyrä esimerkki). Ongelma-alueesta päästävä eroon hakemalla uudet vaatimukset vaiheessa B käytetyille emissiomalleille. Elektronista aktiivisuutta on siis vähennettävä muuttamalla emissiomallin määrittelyitä tai lähetteiden kuvautumista.

6.2. Johtopäätöksiä kehitettyjen menetelmien osalta

Tutkimuksessa on osoitettu, että osajoukon ja joukon elektronista aktiivisuutta sekä elektronisen suojautumisen tasoa arvioivia menetelmiä voidaan määrittää informaatioteoreettisesta nä-

kökulmasta. Menetelmät tuottavat selkeitä mitallisia tuloksia, jotka antavat lisäarvoa erilaisille toimintavaihtoehtojen vertailuille.

Elektronisen suojautumisen keinovalikoimasta keskeisiä esitettyjen arviointimenetelmien kannalta ovat laitteistojen ja lähetteiden identtisyys sekä emissioiden hallinta. Lähetteiden identtisyyden merkitys on ehkäpä kaikkien helpoin elektroniseen suojautumiseen vaikuttava tekijä, jonka teho voidaan selkeästi osoittaa entropian määritelmän avulla. Onhan entropia (epävarmuus) suurimmillaan, kun joukon lähetejakauma on tasajakauma. Menetelmien 1 ja 2 avulla voidaan arvioida lähetteiden identtisyyden vaikutuksia joukon elektronisen suojautumisen tasolle.

Emissioiden hallinnan mallintamiseen on käytössä kolme parametria, jotka ovat emissiomallien siirtymätodennäköisyydet, symbolinopeudet ja kuvautumistodennäköisyydet. Säätämällä näitä parametreja ja hyödyntämällä menetelmiä 3 ja 4, voidaan tuottaa vertailukelpoisia tuloksia eri olosuhteista. Luvussa 5.4.1 (ks. myös luku 6.1.2) on hahmoteltu kokonaan uudenlaista EMCON-kriteeristöä, joka perustuisi joukon tuottaman informaation määrään. Sinänsä tällainen lähestymistapa mahdollistaisi hyvinkin selkeiden ja yksityiskohtaisten EMCON-ohjeistuksien laadinnan ja toteuttamisen. On kuitenkin huomattava luvussa 5.4.4 esitetyt rajoitteet menetelmien kyvystä kuvata tiedustelujärjestelmän todellista toimintaa. Tämä saattaa, johtaa johtopäätöksiin, jotka eivät käytännössä toimi.

Tällä hetkellä lähes kaikkien esiteltyjen menetelmien laajamittaisempi ja tehokas hyödyntäminen edellyttää jatkotutkimuksia ja edelleen sopivien analysaattoreiden tai simulaattoreiden kehittämistä.

6.3. Tutkimuksen ja tutkimustulosten luotettavuuden arviointia

Viitemallina menetelmien kehittämiselle ovat tässä työssä toimineet informaatioteoreettiset määritelmät (vrt. luku 1.3). Tällainen viitemallin määrittely on varsin laaja eikä varsinaisesti ole sidottu teknisiin standardeihin, malleihin tai arkkitehtuureihin. Laaja määrittely on jättänyt tutkijalle mahdollisuuden valita käytettäviä informaatioteoreettisia työkaluja kuhunkin tilanteeseen sopivalla tavalla. Käytettyjen työkaluja ovat olleet erityisesti: entropian määritelmä, yhtenäisinformaatio, suhteellinen entropia, ehdollinen entropia ja informaation yhteenlaskettavuus. Kuvattaessa emissiomalleja on lisäksi hyödynnetty stokastisten prosessien (ml. Mar-

kov ketjujen) määritelmiä. Kaikki nämä työkalut on määritelty lähdekirjallisuudessa matemaattisesti ja muine perusteluineen. Työkalut on tarvittavilta osin esitelty luvussa 3.

Pääkirjallisuutena työssä ovat olleet [62], [63], [55] ja [36], joita alkuperäisimmiksi lähteet eivät voi tulla. Näissä julkaisuissa esitetyt määritelmät ovat edelleen valideja ja niitä on hyödynnetty ja hyödynnetään tänäkin päivänä laajasti erilaisissa tutkimuksissa. Erityisesti on syytä korostaa Shannonin teorioiden merkitystä informaatioteorian fundamentaaleina määritelminä. Shannonin työn merkitykseen voi perehtyä esimerkiksi julkaisun [23] avulla.

Yllä esitetyn perusteella voidaan todeta, että esiteltyjen menetelmien matemaattinen perusta on varsin luotettava. Muutamien yksityiskohtien osalta lähdekirjallisuudesta ei ole löytynyt valmista todistettua määritelmää. Tällöin menetelmien kehittämisen kannalta tarpeelliset määritelmät ja matemaattiset lauseet on muodostettu tutkijan toimesta. Lauseet ja niiden todistukset on esitelty liitteissä. Menetelmien matemaattista perustaa tarkasteltaessa on syytä aina muistaa perusolettamukset, joiden oletetaan olevan voimassa. Näitä olettamuksia on kirjattu lukuun 5.4.4.

Vaikka menetelmien teoreettinen mallinnus ja toteuttaminen vaikuttaisivat luotettavilta, ei tämä takaa kehitettyjen menetelmien olevan sellaisenaan käyttökelpoisia käytännössä sovellettaviksi. Ainakin voidaan epäillä, että saadut tulokset eivät vastaa todellisuutta. Erityisesti tämä saattaa olla menetelmien 3 ja 4 ongelma, koska perusta näiden menetelmien käytettävyydelle luodaan emissiomallin kautta. Toisin sanoen jo tarkastelujen lähtökohtana olevaa todellisuutta yritetään kuvata keinotekoisella mallilla. Tässä työssä nämä mallit perustuvat vakaisiin stokastisiin prosesseihin ja erityisesti Markov ketjuihin. Prosessin vakaus tarkoittaa, että prosessi saavuttaa vakaan todennäköisyysjakauman, kun se on ollut toiminnassa äärettömän pitkän ajan (ks. luku 3.3.1). Todelliset järjestelmät eivät kuitenkaan ole ikinä täysin vakaita, koska kaikki käytännölliset laitteet, yksilöt ja prosessit voivat toimia tai olla olemassa vain äärellisiä aikoja [23]. Menetelmät 3 ja 4 antavat näin ollen tarkkoja tuloksia emissiomallin suhteen. On kuitenkin muistettava, että emissiomallilla voidaan kuvata todellisuutta vain rajoitetusti.

Emissiomallin kuvaamisessa on sovellettu lähteessä [62] esitettyä Markov prosesseihin perustuvaa mallinnusta. Markov ketjujen etuna on se, että entropian määrä on erityisen helposti laskettavissa [16, s. 77]. Joidenkin näkökantojen mukaan Markov prosessit ovat liian yksinkertaisia, jotta niillä kyetään mallintamaan taistelua yleisesti [42, s. 12]. Tämän työn puitteissa ei

ole tutkittu mahdollisuuksia soveltaa emissiomallin kuvaamisessa esimerkiksi yleispätevämpiä ergodisten informaation lähteiden määritelmiä[15].

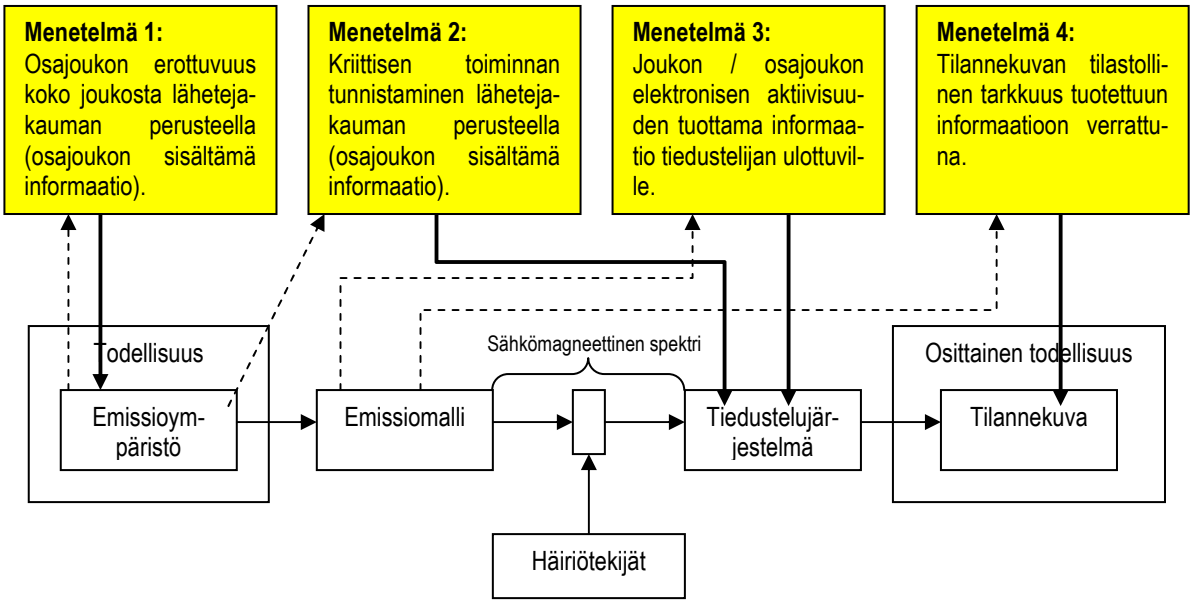
Menetelmä 1 tarjoaa mahdollisuuden tuottaa suoraan todellisuutta vastaavia tuloksia. Menetelmän 2 osalta tulokset riippuvat hyvin paljon siitä, millaisiksi maantieteelliset solut asetetaan. Tämän menetelmän antamien tulosten luotettavuutta ja käyttökelpoisuutta tulisi tutkia jollain rinnakkaisella tutkimusmenetelmällä.

Informaation yhteenlaskettavuudella on suuri merkitys tässä esiteltyjen menetelmien käytön kannalta ja sitä voidaan hyödyntää, kun pidetään tarkasti kiinni erilaisten informaation osien riippumattomuudesta. Luvun 5.4.4 lopussa osoitettiin, että tässä työssä käytetty mallinnus ei huomioi tiedustelujärjestelmässä mahdollisesti olevaa älyä, joka voi tuottaa joltain tasolta katsottuna täydellisempää tilannekuvaa, kuin mihin vastaanotetun informaation määrä antaisi edellytyksiä. Johtopäätösten teko vaatii jonkinasteista informaation merkityksen ymmärtämistä, vaikka sinänsä itse informaation sisältöön (esim. viestin) ei päästäisikään käsiksi. Johtopäätösten teko lähestyy siis informaation semantiikan analysointia, joka rajattiin tämän tutkimuksen ulkopuolelle. On syytä muistaa, että tässä työssä kehitetyt menetelmät nojaavat puhtaasti tilastolliseen informaatiokäsitykseen ja siten ne eivät kykene kuvaamaan luotettavasti tiedustelujärjestelmän suorituskykyä muuta kuin tilastollisen lähestymistavan näkökulmasta.

6.4. Jatkotutkimustarpeita ja -mahdollisuuksia

Jatkotutkimustarpeita ja -mahdollisuuksia kartoitetaan kuvassa 6.4 esitettyyn tilannekuvan muodostumista mallintavaan järjestelmään sitoen. Tähän lukuun on koottu myös aikaisemmissa luvuissa esitetyt tarpeet erilaisista lisäselvityksistä. Luvun alussa keskitytään arvioimaan tärkeimpiä jatkotutkimustarpeita kuvassa 6.4 esitetyn mallin kokonaisuuden kannalta. Tämän jälkeen kartoitetaan kuhunkin vaiheeseen tai menetelmään liittyvät tarpeet.

[15] Esimerkiksi McMillanin yleistykset [43].



Kuva 6.4: Tilannekuvan muodostumista mallintava järjestelmä ja kehitettyjen arviointimenetelmien sijoittuminen sen eri vaiheisiin.

Tässä työssä johdetut menetelmät ovat luonteeltaan varsin teoreettisia. Kohtuullisella joukolla esimerkkejä on pyritty osaltaan osoittamaan, että menetelmillä on mahdollista tuottaa käytäntöön sidottuja tuloksia. Menetelmiä ei kuitenkaan ole millään tavalla verifioitu kattavilla testauksilla tai simuloinneilla. Kaikkia esiteltyjä menetelmiä tulisi testata käytännöllisiin tilanteisiin sitoen ja edelleen arvioida niiden käyttökelpoisuutta ja mahdollisuuksia jatkokehittämiselle. Erityisesti menetelmien 2, 3 ja 4 laajamittainen hyödyntäminen edellyttäisi sopivien analysaattoreiden tai simulaattoreiden kehittämistä.

Kokonaisuuden kannalta olisi tärkeää kyetä luomaan algoritmi tai mallinnus, joka arvioisi joukon elektronista aktiivisuutta ja elektronisen suojautumisen tasoa mahdollisimman monesta näkökulmasta samanaikaisesti. Karkeasti ottaen tällainen mallinnus yhdistäisi esimerkiksi tässä työssä esitellyt neljä menetelmää ja tuottaisi lopputulokseksi osajoukkoa ja joukkoa kuvaavia elektronisen suojautumisen tason mitallisia ”arvosanoja”. Tässä työssä ei varsinaisesti ole pyritty yhdistämään esiteltyjä keinoja menetelmäksi, joka ottaisi kerralla huomioon kaikki arviointiin liittyvät tekijät. Alustavasti on kuitenkin hahmoteltu mahdollisuuksia yhdistää lähetetodennäköisyydet emissiomalleihin. Tällöin kunkin emissiomallin tuottamaa symbolia painotettaisiin tätä symbolia vastaavalla lähetetodennäköisyydellä (P_{Li}). Näin aikaan saatu emissioympäristön entropia ottaisi siis huomioon sekä lähettimen suhteellisen yleisyyden/harvinaisuuden ko. joukossa, että lähettimen tilastollisen aktiivisuuden ympäristöönsä nähden. Tällöin lähteen entropia laskettaisiin (vrt. luku 4.3.2)

$$H_s = \sum_i P_{Li} p_i \log \frac{1}{p_i} \text{ tai} \quad (6.1)$$

$$H_s = \sum_{i,j} P_{Li} \mu_i P_{ij} \log \frac{1}{P_{ij}}. \quad (6.2)$$

Muitakin lähestymistapoja yhtenäismallin muodostamiselle on varmasti löydettävissä. Yhtenäismallin tai käyttökelpoisen algoritmin muodostaminen on selkeä jatkotutkimusmahdollisuus etenkin, jos informaatioteoreettiseen näkökulmaan perustuvia arviointimenetelmiä halutaan kehittää käytännöllisiksi työkaluiksi.

Emissiomalliin liittyvä jatkotutkimus on myös erityisen tärkeä seikka, mikäli esitetyillä menetelmillä halutaan tuottaa käytännöllisiä tuloksia. Ensinnäkin tulee tutkia, voidaanko todellisia joukkoja ja radioverkkoja edes jotakuinkin realistisesti mallintaa stokastisten prosessien ja erityisesti Markov ketjujen avulla. Kuten luvussa 6.3 on todettu, täydellinen todellisuuden kuvaaminen tällaisilla prosesseilla on mahdotonta. Näin ollen on tärkeää kyetä edes karkeasti määrittämään myös se, mikä on hyväksyttävä poikkeaman taso. Todennäköisesti yksi osajoukko tarvitsee useita erilaisia emissiomalleja erilaisiin tilanteisiin (vrt. luku 5.4.4). Eräs emissiomalleihin liittyvä jatkotutkimusmahdollisuus on pyrkiä laajentamaan informaation lähteen mallinnusta yleisemmin määriteltyihin stokastisiin prosesseihin pelkkien Markov prosessien sijasta.

Erilaiset häiriötekijät voidaan kaikilta osin huomioida kuvautumistodennäköisyyksissä, jotka muodostuvat sieppaus-, ilmaisu- ja hyödyntämistodennäköisyyksien tulona. Ilmaisu- ja hyödyntämistodennäköisyyksien määrittämiseksi on tässä työssä esitelty selkeät, joskin hieman rajoittuneet, periaatteet (ks. luku 4.3.3). Sieppaustodennäköisyyksien osalta todettiin, että yksityiskohtiin menevien laskelmien sijasta priorisoidaan emissioympäristön kohteet ja oletetaan, että tiedustelija käyttää resurssejaan eniten tärkeimpien kohteiden sieppaamiseen. Tällainen priorisointi ja siitä seuraava parametrointi edellyttää jatkoselvityksiä, joissa arvioidaan organisaatio- ja taistelutilannekohtaisesti tiedustelijan kannalta mielenkiintoisimmat kohteet.

Erilaisia hajaspektritekniikoita hyödyntävät lähettimet eivät sinänsä vaikuta mitenkään kehitettyihin elektronista aktiivisuutta arvioiviin menetelmiin. Näiden tekniikoiden vaikutus näkyy ennen kaikkea sieppaus- ja ilmaisutodennäköisyyksissä sekä mahdollisesti myös hyödyntämistodennäköisyyksissä. Näin ollen tällä saralla mahdollisesti tehtävä jatkotutkimus tarkentaisi mallinnusta kuvautumistodennäköisyyksien osalta.

Menetelmät 2 ja 3 arvioivat hieman eri näkökulmista kuinka paljon informaatiota tiedustelujärjestelmällä on käytettävissään. Menetelmän 2 osalta jatkotutkimustarpeiksi on jo todettu etenkin maantieteellisten solujen koon analysointi sekä menetelmällä tuotettujen tulosten vertailu mahdollisesti joihinkin toiseen tutkimusmenetelmään tai lähestymistapaan sitoen. Menetelmään 3 liittyvät jatkotutkimustarpeet liittyvät jo mainittuihin emissiomallien ja kuvautumistodennäköisyyksien kehittämiseen sekä tarkentamiseen.

Myös menetelmän 4 osalta emissiomallien ja kuvautumistodennäköisyyksien jatkotutkimus on oleellista. Lisäksi menetelmän hyödyntäminen käytäntöön edellyttäisi, että jakaumien epäsovituksille (eli tilannekuvan tilastolliselle tarkkuudelle) kyetään määrittämään joitain hyväksyttäviä raja-arvoja. Toisin sanoen on kyettävä määrittämään millainen suhteellisen entropian arvon tulee olla, jotta tuotettuun tilannekuvaan ollaan tyytyväisiä.

Tiedustelujärjestelmän toiminta ja tilannekuvan muodostaminen tarjoavat laajempiakin jatkotutkimusmahdollisuuksia, jotka eivät välttämättä rajoitu vain elektronisen sodankäynnin alueelle. Kuten edellä on todettu, tässä työssä esitellyt menetelmät kuvaavat vain tilastolliseen näkökulmaan perustuvaa informaation määrää, joka on tiedustelujärjestelmään vastaanotettavissa ja siten käytettävissä tilannekuvan muodostamiseen. Tiedustelujärjestelmän suorituskyvyn osalta ei huomioida tekijöitä, jotka saattava kyetä muodostamaan tilannekuvaa tai -ymmärrystä, joka on laadultaan parempaa, kuin vastaanotetun informaation määrä antaisi odottaa. Toisaalta tilanne voisi olla myös toisin päin, eli informaation määrä on suurempi, kuin mitä tilannekuvan laatu on. Tämän ongelmanasettelun kautta pääsemme käsiksi luvussa 4.3.4 esiteltyyn tiedustelujärjestelmän absoluuttisen kapasiteetin määritelmään. Eräs mielenkiintoinen, joskin erinomaisen haastava, tutkimuskohde voisi olla tämän absoluuttisen raja-arvon löytäminen.

Tämän työn varsinaisena tarkoituksena ei ole ollut tuottaa johtopäätöksiä siitä, miten elektronista suojautumista tulisi käytännössä toteuttaa. Tässä esitellyt menetelmät tarjoavat tämän tyyppiselle tutkimukselle mahdollisuuksia. Esimerkkeinä tutkittavista aihealueista voisivat olla: a) Joukkojen hajauttamisen / hajauttamattomuuden merkitys elektronisen aktiivisuuden ja elektronisen suojautumisen kannalta. b) Kaupallisten tietoliikennelaitteiden hyödyntäminen joukon viestivälineinä. Vaikutusten tarkastelu elektronisen aktiivisuuden ja elektronisen suojautumisen näkökulmasta.

6.5. Loppupäätelmät

Informaatioteoreettinen näkökulma tarjoaa aikaisempaa monipuolisemmat mahdollisuudet arvioida sotilasjoukkojen organisaatioita, käyttöperiaatteita ja toimintavaihtoehtoja elektronisen suojautumisen osalta. Yksikäsitteiset ja mitalliset tulokset mahdollistavat erilaisten olosuhteiden ja vaihtoehtojen vertailun. Tämä onkin esiteltyjen menetelmien suurin anti operatiivista suunnittelua, operaatioanalyysia sekä tutkimus- ja kehittämistoimintaa ajatellen. Kuten edellä on todettu (ks. luku 6.3), taistelukentän mallintaminen absoluuttisesti oikein riittävällä tarkkuudella on lähes mahdoton tai ainakin hyvin paljon resursseja vaativa tehtävä. Tällöin absoluuttisesti oikeiden tulosten tuottaminen arviointimenetelmillä on myös lähes mahdotonta. On kuitenkin todennäköistä, että epätarkkuudet mallinnuksessa vertailtavien olosuhteiden välillä voidaan pitää ainakin jotakuinkin vakioina. Juuri tällaisissa tilanteissa esitellyt menetelmät antavat tuloksia, joita hyödyntämällä erilaiset vaihtoehdot ja tilanteet voidaan arvottaa paremmuusjärjestykseen. Tämä arvottaminen antaa mahdollisuuden tukea päätöksentekoa, joka on operaatioanalyysin keskeinen tavoite [42, s. 5]. Ottamalla huomioon vain esimerkiksi kohteiden ilmaistavuuteen liittyvät tekijät (kentänvoimakkuusanalyysit), ei välttämättä saada tuotettua riittävää eroa erilaisten vaihtoehtojen ja tilanteiden välille.

Luvussa 1.2 tutkimuksen loppuasetelmalle kirjattiin seuraavasti:
Loppuasetelmassa on päästy tilanteeseen, jossa tutkimuskysymyksiin on vastattu ja on arvioitu miltä osin menetelmien hyödyntäminen osana operatiivista suunnittelua tai operaatioanalyysia on sellaisenaan mahdollista ja miltä osin menetelmien hyödyntäminen edellyttää jatkotutkimuksia sekä kehittämistä.

Voidaan todeta, että tutkimuskysymyksiin on vastattu ja arvioitu kehitettyjen menetelmien hyödynnettävyyttä operatiivisen suunnittelun ja operaatioanalyysin kannalta. Menetelmien teoreettinen pohja on luotettava. Suurimmaksi kysymysmerkiksi jää se, miten hyvin ja helposti menetelmät ovat hyödynnettävissä käytännön toimintaympäristöön. Tähän liittyviä jatkotutkimustarpeita on katselmoitu edellä. Jatkotutkimusmahdollisuuksiin kirjattiin myös laajempia kokonaisuuksia, kuin mitä tässä esiteltyjen menetelmien kehittäminen edellyttää. Informaatioteoreettista näkökulmaa kannattaa harkita jatkossakin käytettäväksi erilaisten elektronisen sodankäynnin toimintakenttää käsittelevien tutkimusten lähestymistapana.

LÄHTEET

[1] Aczél, J. & Daróczy, Z.: On Measures of Information and Their Characterizations. Academic Press Inc., New York NY 1975. ISBN 0-12-043760-0.

[2] Adams, Robert, A.: Calculus – a complete course, 3rd edition. Addison – Wesley Publishers Ltd., Canada 1995. ISBN 0-201-82823-5

[3] AITACS – Advanced Integrated Transportable COMINT System. Esittelymateriaali. IAI ELTA Systems Ltd., Israel. Esite ladattu 24.7.2010 www.iai.co.il.

[4] Ash, Robert: Information Theory. Interscience Publishers / John Wiley & Sons, USA 1967.

[5] Bar-Hillel, Yehoshua & Carnap, Rudolf: Semantic Information. The British Journal for the Philosophy of Science, Vol. 4, No. 14, August 1953. pp. 147 – 157.

[6] Benson, Craig; Frater, Michael; Ryan, Michael: Tactical Electronic Warfare. Argos Press, 2007. ISBN 978-1-921138-04-1

[7] Borden, Andrew: The Design and Evaluation of Situation Assessment Strategies. Information & Security, Vol. 1, No. 1, 1998, pp. 63 – 74.

[8] Borden, Andrew: Human Intuition and Decision-Making Systems I. Information & Security, Vol.1, No. 2, 1998, pp. 67 – 72.

[9] Borden, Andrew: The Dialectics of Information – a framework. Information & Security, Vol. 4, 2000.

[10] Borden, Andrew: The Shannon-Hartley Theorem as a Unifying Principle in Electronic Warfare and Information Warfare. Transactions of the AOC, Vol. 1, No. 1, pp. 43 – 49, October 2004.

[11] Borden, Andrew: Classification using conditional probabilities and Shannon's definition of information. Proceedings of the 2007 International Lisp Conference, 2007.

[12] B-GL-358-001/FP-001 Land Force Information Operations – Electronic Warfare. Canada, March 2004.

[13] Clarkson, I.V.L; Perkins, J.E; Mareels, I.M.Y: Number Theoretic Solutions to Intercept Time Problems. IEEE Transactions on Information Theory, Vol. 42, No. 3, May 1996.

[14] Clarkson, I.V.L: The Farey Series in Synchronisation and Intercept-Time Analysis for Electronic Support. Transactions of the AOC, Vol. 1, No. 1, pp. 7 - 28, October 2004.

[15] Clarkson, I.V.L: The Arithmetic of Receiver Scheduling for Electronic Support. In Proceedings of Aerospace Conf., Vol 5, March 2003.

[16] Cover, Thomas M. & Thomas, Joy A.: Elements of Information Theory, 2nd edition. John Wiley & Sons Inc., Hoboken NJ 2006. ISBN-10 0-471-24195-4

[17] Department of Defense Interface Standard Electromagnetic Environmental Effects Requirements For Systems (MIL-STD-464A), December 2002.

[18] Digital HF/VHF/UHF Scanning Direction Finder R&S DDF 0xA. Esittelymateriaali. Rohde&Schwarz, Saksa. Esite ladattu 24.7.2010 www.rohde-schwarz.com.

[19] Ekberg, Jan & Halme, Seppo J.: Informaatioteoria, 2. painos. Otakustantamo, Otapaino, Espoo 1978. ISBN 951-671-122-7.

[20] Elliot, Linda & Borden, Andrew: Human Intuition and Decision-Making Systems II. Information & Security, Vol.2, 1999.

[21] Esmeralda XE – Compact Spectrum Monitoring Equipment. Järjestelmän esittelymateriaali. Thales, Land & Joint Systems Division, Ranska. Esite ladattu 24.7.2010 www.thalesgroup.com.

[22] Frater, Michael R. & Ryan Michael: Electronic Warfare for the Digitized Battlefield. Artech House Inc, Norwood MA 2001. ISBN 1-58053-271-3

[23] Gallager, Robert, G.: Claude E. Shannon – A Retrospective on His Life, Work, and Impact. IEEE Transactions on Information Theory, Vol. 47, No. 7, November 2001.

[24] Hall, David, L. & Llinas, James: An Introduction to Multisensor Data Fusion. Proceedings of the IEEE, Vol. 85, No. 1, January 1997.

[25] Hancock, John C. & Wintz, Paul A.: Signal Detection Theory. McGraw-Hill Inc., USA 1966.

[26] Hintikka, Jaakko & Suppes, Patrick (editors): Information and Inference. D. Reidel Publishing Company, Dordrecht, Holland 1970.

[27] Hämäläinen, Juhani S. (editor): Lanchester and Beyond – A Workshop on Operational Analysis Methodology, 16 October 2006, Finnish Defence Forces Technical Research Center, Riihimäki. Edita Prima Oy, Helsinki 2006. ISBN 951-25-1707-8.

[28] International Telecommunication Union – Radiowave propagation.
http://www.itu.int/rec/R-REC-P/en
Sivustoilta löytyy erilaisia suosituksia radioaaltojen etenemisen mallintamiseksi.

[29] Joint Publication 3-51, Joint Doctrine for Electronic Warfare, 7 April 2000.

[30] Kari, Mikko; Hakala, Arto; Pääkkönen, Elisa; Pitkänen, Markku (toim.): Sotatekninen arvio ja ennuste 2025 (STAE 2025), osa 2 – Puolustusjärjestelmien kehitys. PVTT, julkaisusarja 15. Edita Prima Oy, Helsinki, 2008. ISBN 978-

951-25-1890-6

[31] Kenttälinkkiopas 1985. Sisälähetysseuran kirjapaino Raamattutalo, Pieksämäki 1985. ISBN 951-25-0327-1

[32] Kenttäohjesääntö – Yleinen osa. Puolustusjärjestelmän toiminnan perusteet. Pääesikunta, Suunnitteluosasto, Edita Prima Oy, Helsinki 2007. ISBN 978-951-25-1744-2

[33] Kosola, Jyri & Solante, Tero: Digitaalinen taistelukenttä – Informaatioajan sotakoneen tekniikka, 2. painos. Maanpuolustuskorkeakoulu, tekniikan laitos. Edita Prima Oy, Helsinki 2003. ISBN 951-25-1449-4

[34] Kosola, Jyri & Jokinen, Janne: Elektroninen sodankäynti, osa 1 – taistelun viides dimensio. Maanpuolustuskorkeakoulu, tekniikan laitos. Edita Prima Oy, Helsinki 2004. ISBN 951-25-1554-7.

[35] Kujala, Markku: Naval Stealth Technologies. Artikkeli J Jormakan ja A Rissasen toimittamassa teoksessa State-of-the-Art in Sensors. Maanpuolustuskorkeakoulu, Sotatekniikan laitos, Edita Prima Oy, Helsinki 2006. ISBN 951-25-1650-0.

[36] Kullback, S. & Leibler, R.A.: On Information and Sufficiency. The Annals of Mathematical Statistics 22, 1951

[37] Kullback, Solomon: Information Theory and Statistics. John Wiley & Sons Inc, New York, USA 1959.

[38] Kuosmanen, Petteri: Taktisten ad hoc-radioverkkojen toteuttamismahdollisuudet erilaisissa toimintaympäristöissä. Maanpuolustuskorkeakoulu, Tekniikan laitos, Edita Prima Oy, Helsinki 2004. ISBN 951-25-1562-8. Julkaisu perustuu Kuosmasen laatimaan yleisesikuntaupseerikurssin diplomityöhön (heinäkuu 2004).

[39] Kuusisto, Rauno: Elektroninen sodankäynti johtamissodankäynnin välineenä. Artikkeli. Johtamissodankäynti, Maanpuolustuskorkeakoulu, Taktiikan laitos, Edita Oy, Helsinki, 2000. ISBN 951-25-1187-8

[40] Lafrance, Pierre: Fundamental Concepts in Communication. Prentice-Hall Inc., Englewood Cliffs, New Jersey 1990. ISBN 0-13-335738-4

[41] Lappalainen, Esa & Jormakka, Jorma (toim.): Tekniset tutkimusmenetelmät Maanpuolustuskorkeakoulussa. Maanpuolustuskorkeakoulu, Tekniikan laitos, Edita Prima Oy, Helsinki 2004. ISBN 951-25-1540-7

[42] Lehtinen, Matti: Operaatioanalyysia sotilaille. Maanpuolustuskorkeakoulu, Tekniikan laitos, Edita Prima Oy, Helsinki 2003. ISBN 951-25-1461-3

[43] McMillan, Brockway: The Basic Theorems of Information Theory. The Annals of Mathematical Statistics, Vol. 24, pp. 196 – 219, 1953.

[44] Meerkat-SA ESM/ELINT system. Esittelymateriaali. Thales, Aerospace Division, Iso-Britannia. Esite ladattu 22.9.2009 www.thalesgroup.com.

[45] Meerkat-S Mobile ESM/ELINT system. Esittelymateriaali. Thales, Aerospace Division, Iso-Britannia. Esite ladattu 22.9.2009 www.thalesgroup.com.

[46] Mellin, Ilkka: Todennäköisyyslaskenta – Satunnaismuuttujat ja todennäköisyysjakaumat. http://math.tkk.fi/opetus/sovtoda/oppikirjat/TodLaskSatMuutjaJak.pdf , viitattu 26.7.2011.

[47] Myllylä, Kari & Korteslahti, Niina: Matematiikan perusteet taloustieteilijöille 2. Luentomoniste, Oulun yliopisto, Matemaattisten tieteiden laitos, kevät 2011. http://math.oulu.fi/materiaalit/luentorungot/MPTT2_uusi.pdf. Viitattu 30.6.2011.

[48] Neri, Filippo: Introduction to Electronic Defense Systems, 2nd edition. Artech House inc., Norwood MA 2001. ISBN 1-58053-179-2

[49] Parsons, J. D.: The Mobile Radio Propagation Channel, 2nd edition. John Wiley & Sons Ltd.: Chichester, England 2000. Online ISBN 0-470-84152-4

[50] Parzen, Emanuel: Stochastic Processes. Holden-Day Inc., San Francisco CA, 1962.

[52] Poisel, Richard A.: Electronic Warfare Target Location Methods. Artech House Inc., Norwood MA, 2005. ISBN 1-58053-968-8

[53] Poisel, Richard A.: Introduction to Communication Electronic Warfare Systems, 2nd edition. Artech House Inc, Norwood MA 2008. ISBN 978-1-59693-452-8

[54] Pääkkönen, Matti: A:sta O:hön – Suomen yleiskielen kirjaintilastot. Kielikello 1/1991 s. 3. Artikkeliin viitattu 6.11.2010 http://www.cs.tut.fi/~jkorpela/kielikello/kirjtil.html.

[55] Rényi, Alfréd: On Measures of Entropy and Information. Proceedings of the 4th Berkeley Symposium on Mathematics, Statistics and Probability 1960, pp. 547 – 561. Julkaistu 1961.

[56] Rényi. Alfréd: Probability Theory. North-Holland publishing company, Amsterdam 1970. ISBN 7204-2360-0

[57] Ross, Sheldon M.: Introduction to Probability Models, 4th edition. Academic Press Inc, San Diego CA, 1989.

[58] Ryan, Michael J. & Frater, Michael R.: Tactical Communications for the Digitized Battlefield. Artech House Inc, Norwood MA 2002. ISBN 1-58053-323-x.

[59] Sarkar, T. K.; Ji, Zhong; Kim, Kyungjung; Medouri, A; Salazar-Palma, M: A Survey of Various Propagation Models for Mobile Communication. IEEE Antennas and Propagation Magazine, Vol. 45, No.3, June 2003.

[60] Saukkonen, Pauli; Haipus, Marjatta; Niemikorpi, Antero & Sulkava, Helena: Suomen kielen taajuussanasto. WSOY, Porvoo 1979. ISBN 9510090603.

[61] Schleher, D. Curtis: Electronic Warfare in the Information Age. Artech House Inc, Norwood MA 1999. ISBN 0-89006-526-8

[62] Shannon, Claude E.: A Mathematical Theory of Communication. The Bell System Technical Journal, Vol. 27, pp. 379-423, 623-656, July, October, 1948. Tässä työssä on käytetty uudelleen painettua versiota kyseisestä julkaisusta. Viitteissä käytetyt sivunumeroinnit ovat uudemman version mukaisia, eivätkä noudattele alkuperäisiä julkaisuja.

[63] Shannon, Claude E. & Weaver, Warren: The Mathematical Theory of Communication. The University of Illinois Press, Urbana 1949. Reprinted 1963.

[64] Taylor, Robert J. Jr: Heavy Division Organic Signals Intelligence (SIGINT) – Added Value or Added Baggage. Monograph, School of Advanced Military Studies, United States Army Command and General Staff College, Fort Leavenworth, Kansas, December 1996.

[65] Tolvanen, Pasi; Hemminki, Petteri; Mustonen, Mikko: Joustavan vaatimustenhallinnan soveltaminen emissioidenhallintakonseptin luomiseen. Tiede ja Ase, Suomen Sotilastieteellisen Seuran vuosijulkaisu N:o 67. Multiprint Oy, Vantaa 2009. ISBN 978-951-96314-7-9

[66] Top Scan ESM/ELINT system. Esittelymateriaali. Rafael, Systems Division, Israel. Esite ladattu 22.9.2009 www.rafael.co.il.

[67] Torrieri, Don J.: Principles of Secure Communication Systems, 2nd edition. Artech House Inc., Norwood MA 1992. ISBN 0-89006-555-1

[68] Vaccaro, Dennis D.: Electronic Warfare Receiving Systems. Artech House Inc., Norwood MA 1993. ISBN 0-89006-543-8

[69] Wideband V/UHF COMINT/DF System Family – EL/K-7036. Esittelymateriaali. IAI ELTA Systems Ltd, Israel. Esite ladattu 24.7.2010 www.iai.co.il.

[70] Wiley, Richard G: Electronic Intelligence: The Interception of Radar Signals. Artech House Inc, Dedham MA 1985. ISBN 0-89006-138-6

[71] Wiley, Richard G.: The Analysis of Radar Signals, 2nd edition. Artech House Inc, Norwood MA 1993. ISBN 0-89006-592-6

[72] Wiley, Richard G.: ELINT: The Interception and Analysis of Radar Signals. Artech House Inc., Norwood MA 2006. ISBN 978-1-58053-926-5.

LIITELUETTELO

MATEMAATTISET PERUSTELUT LUKUUN 4.2.3

1. Symbolien kuvautumista ohjaavat perusmääritelmät

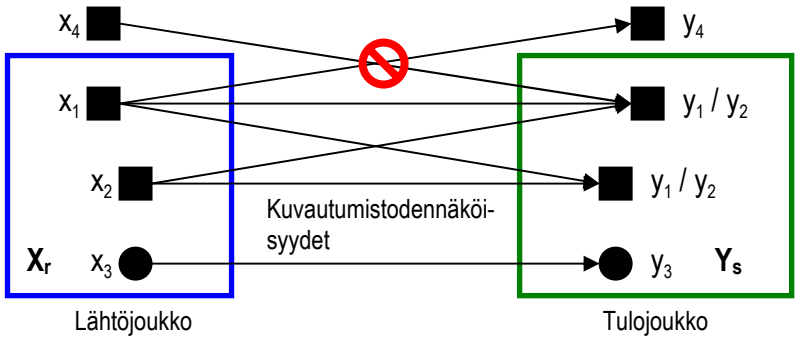
Määritelmä L1.1
Kuvautumista lähtöjoukosta X_k tulojoukkoon Y_k rajoitetaan seuraavilla säännöillä:

- $x_i \in X_r \mapsto y_j \in Y_s$ vain jos $r = s$ ja
- $x_i \in Lt \mapsto y_j \in Lu$ vain jos $t = u$ ja (*Ln* on lähetekategorian tunnus)
- $x_i \in X_r$ kuvautuu aina kaikiksi $y_j \in Y_s$, mikäli kaksi ensimmäistä ehtoa täyttyvät.
- Lähtöjoukon symboleiden indeksijoukko muodostetaan: $i \in \{g,...,h\}$, missä joukko $\{g,...,h\}$koostuu luonnollisista luvuista. Tulojoukon symboleiden indeksijoukko on aina identtinen lähtöjoukon symboleiden indeksijoukkoon nähden eli $j \in \{g,...,h\}$.

Tulkinta:

- Joukkoon X_r kuuluva symboli kuvautuu vain juuri tätä lähtöjoukkoa vastaavaan tulojoukkoon Y_s. Kuvautuminen johonkin muuhun tulojoukkoon ei ole mahdollista. Ei ole myöskään mahdollista, että tulojoukkoon Y_s kuvautuisi symboleita jostain muusta lähtöjoukosta.
- Lähtöjoukon symboli x_i voi kuvautua vain samaan lähetekategoriaan kuuluviksi tulojoukon symboleiksi y_j. Katso lähetekategorian määritelmä määritelmästä L1.3.
- Lähtöjoukon symboli x_i kuvautuu samalla todennäköisyydellä miksi tahansa kaksi ensimmäistä ehtoa täyttäväksi tulojoukon symboliksi y_j. Kuvautuminen on tarkemmin esitetty määritelmässä L1.2.
- Tulojoukon symboleiden lukumäärä ja indeksointi on aina sama, kuin lähtöjoukon.

Samaan soluun kuuluvat ja samaan lähetekategoriaan kuuluvat symbolit voivat kuvautua keskenään ristiin. Kokonaan uusien symbolien syntyminen tai olemassa olevien häviäminen ei ole mahdollista. Tilannetta on havainnollistettu kuvassa L1.1.



Kuva L1.1: Lähtöjoukon symbolien kuvautuminen tulojoukon symboleiksi.

Määritelmä L1.2
Lähtöjoukon $X_k = \{x_g, x_{g+1},..., x_h\}$ kuvautumista tulojoukkoon $Y_k = \{y_g, y_{g+1},..., y_h\}$ säädellään kuvautumistodennäköisyyksillä c_{ij} seuraavasti

$$c_{ij} = \begin{cases} \dfrac{1}{S^{Ln}} & \text{, kun } x_i \in Lt \text{ ja } y_j \in Lu \text{ ja } t = u \\ 0 & \text{, kun } x_i \in Lt \text{ ja } y_j \in Lu \text{ ja } t \neq u \end{cases}. \qquad \text{(L1.1)}$$

Tässä S^{Ln} on solussa (X_k) olevien samaan lähetekategoriaan kuuluvien symbolien lukumäärä ja *Ln* on lähetekategorian tunnus.

Kaikille lähtöjoukon symboleille x_i pätee lisäksi

$$\sum_{j=g}^{h} c_{ij} = 1, \qquad \text{missä } i = g, g+1, \ldots, h. \qquad \text{(L1.2)}$$

Kuvautumistodennäköisyydet voidaan esittää kuvautumistodennäköisyysmatriisina (kanavamatriisina) **C** seuraavasti

$$C = \begin{pmatrix} c_{gg} & c_{gg+1} & \cdots & c_{gh} \\ c_{g+1g} & c_{g+1g+1} & \cdots & c_{g+1h} \\ \vdots & \vdots & \ddots & \vdots \\ c_{hg} & c_{hg+1} & \cdots & c_{hh} \end{pmatrix}. \qquad \text{(L1.3)}$$

Määritelmä L1.3 - Lähetekategoria
Olkoon $X = \{x_1, x_2, ..., x_m\}$ joukko emissioympäristön lähettimiä, jotka on jaoteltu siten, että samantyyppiset lähettimet ovat peräkkäin. Erotetaan peräkkäin järjestetyt lähettimet osajoukoiksi $X_{L1}, X_{L2}, ..., X_{Lk} \subset X$ siten, että kuhunkin osajoukkoon sisältyy vain yhden tyyppisiä lähettimiä. Lisäksi vaaditaan, että kaikki samantyyppiset lähettimet kuuluvat samaan osajoukkoon. Nyt pätee

$$\bigcap_{n=1}^{k} X_{Ln} = \varnothing \text{ ja } \bigcup_{n=1}^{k} X_{Ln} = X .$$

Näin muodostettuja yksittäisiä osajoukkoja X_{Ln} kutsutaan lähetekategorioiksi. *Ln* on kategorian tunnus.

Määritelmä L1.4 – Lähetetodennäköisyys
Olkoon $X = \{x_1, x_2, ..., x_m\}$ joukko emissioympäristön lähettimiä, jotka voidaan jakaa *k* kappaleeseen lähetekategorioita (ks. määritelmä L1.3). Merkitään kuhunkin osajoukkoon X_{Ln} sisältyvien lähettimien kokonaislukumäärää S_0^{Ln}, missä $n = 1, \ldots, k$. Yksittäisen kategoriaan *Ln* kuuluvan lähettimen todennäköisyys tulla valituksi kaikkien ko. kategoriaan kuuluvien lähettimien joukosta on $1/S_0^{Ln}$. Saatu suhde normalisoidaan koko joukon suhteen jakamalla kategorioiden lukumäärällä *k*. Nyt saadaan

$$P_{Ln} = \frac{1}{kS_0^{Ln}}, \qquad \text{missä } n = 1, \ldots, k \text{ ja } k \neq 0 \text{ sekä } S_0^n \neq 0. \quad \text{(L1.4)}$$

Suhdetta P_{Ln} nimitetään lähetetodennäköisyydeksi ja se kuvaa yksittäisen lähettimen yleisyyttä koko joukossa *X*.

2. Epätäydelliset jakaumat

Määritelmä L1.5
Diskreetti todennäköisyysjakauma $P(X=x_i) = p(x_i)$ ($i = 1, \ldots, n$) on epätäydellinen mikäli

$$\sum_{i=1}^{n} p(x_i) < 1. \qquad \text{(L1.5)}$$

Lause 1: Epätäydelliset jakaumat

Lähtöjoukon $X_k = \{x_g, x_{g+1}, ..., x_h\}$ symboleiden tilastollista jakaumaa kuvataan epätäydellisellä diskreetillä todennäköisyysjakaumalla $P_L(X = x_i) = p(x_i)$, jossa $i = g, \ldots, h$. Tällöin myös vastanottotodennäköisyysjakauma $P(Y = y_j) = p(y_j) = v_j$ ja yhteinen todennäköisyysjakauma $P(X,Y)$ ovat epätäydellisiä.

Todistus:

Muodostetaan lähtöjoukon todennäköisyysjakaumasta todennäköisyysvektori $\mathbf{P_L}$ siten, että

$$P_L = \begin{pmatrix} p(x_g) & p(x_{g+1}) & \cdots & p(x_h) \end{pmatrix}.$$

Vastaanottotodennäköisyydet $p(y_j) = v_j$ saadaan todennäköisyysvektorin $\mathbf{P}_L$ ja kuvautumistodennäköisyysmatriisin $\mathbf{C}$ tulona

$$v_j = P_L C, \qquad \text{missä } v_j = \sum_{i=g}^{h} p(x_i) c_{ij} \text{ ja } j = g, g+1, \ldots, h.$$

Tämän perusteella saadaan

$$\begin{aligned}
v_g &= p(x_g)c_{gg} + p(x_{g+1})c_{g+1g} + \ldots + p(x_h)c_{hg} \\
v_{g+1} &= p(x_g)c_{gg+1} + p(x_{g+1})c_{g+1g+1} + \ldots + p(x_h)c_{hg+1} \\
&\vdots \\
v_h &= p(x_g)c_{gh} + p(x_{g+1})c_{g+1h} + \ldots + p(x_h)c_{hh}
\end{aligned}$$

Lasketaan nyt näiden summa

$$\sum_{j=g}^{h} v_j = p(x_g)c_{gg} + \ldots + p(x_h)c_{hg} + p(x_g)c_{gg+1} + \ldots + p(x_h)c_{hg+1} + p(x_g)c_{gh} + \ldots + p(x_h)c_{hh}\ .$$

Muuttamalla termien järjestystä ja ottamalla yhteiseksi tekijäksi $p(x_i)$ saadaan yllä oleva muotoon

$$\begin{aligned}
\sum_{j=g}^{h} v_j = {} & p(x_g)(c_{gg} + c_{gg+1} + \ldots + c_{gh}) + p(x_{g+1})(c_{g+1g} + c_{g+1g+1} + \ldots + c_{g+1h}) + \ldots \\
& + p(x_h)(c_{hg} + c_{hg+1} + \ldots + c_{hh}).
\end{aligned}$$

Määritelmän L1.2 perusteella tiedämme, että yllä olevassa lausekkeessa summat

$$(c_{gg} + c_{gg+1} + \ldots + c_{gh}) = (c_{g+1g} + c_{g+1g+1} + \ldots + c_{g+1h}) = (c_{hg} + c_{hg+1} + \ldots + c_{hh}) = 1.$$

Näin ollen saadaan

$$\sum_{j=g}^{h} v_j = p(x_g) + p(x_{g+1}) + ... + p(x_h) = \sum_{i=g}^{h} p(x_i) \underbrace{\leq 1}_{\text{Määritelmä Lf.5}} . \qquad \text{(L1.6)}$$

Näin ollen on osoitettu, että vastaanottotodennäköisyysjakauma on epätäydellinen. Lisäksi on osoitettu, että lähtöjoukon todennäköisyysjakauman ja vastaanottojakauman summat ovat yhtä suuria. ■

Seuraavaksi paneudutaan yhteistodennäköisyysjakaumaan $p(x_i, y_j)$, joka on määritelty

$$p(x_i, y_j) = p(x_i)\, p(y_j \mid x_i) .$$

Tässä ehdollinen todennäköisyys $p(y_j \mid x_i)$ ilmoittaa millä todennäköisyydellä tiedetty symboli x_i kuvautuu symboliksi y_j. Ehdollinen todennäköisyys on siis sama, kuin kuvautumistodennäköisyys c_{ij}. Nyt voidaan lausua

$$\sum_{i=g}^{h}\sum_{j=g}^{h} p(x_i, y_j) = \sum_{i=g}^{h}\sum_{j=g}^{h} p(x_i) c_{ij} = p(x_g) c_{gg} + ... + p(x_g) c_{gh} + ... + p(x_h) c_{hg} + ... + p(x_h) c_{hh}$$
$$= p(x_g)(c_{gg} + ... + c_{gh}) + p(x_{g+1})(c_{g+1g} + ... + c_{g+1h}) + ... + p(x_h)(c_{hg} + ... + c_{hh}) .$$

Määritelmän L1.2 perusteella tiedämme, että yllä olevassa lausekkeessa summat

$$(c_{gg} + c_{gg+1} + ... + c_{gh}) = (c_{g+1g} + c_{g+1g+1} + ... + c_{g+1h}) = (c_{hg} + c_{hg+1} + ... + c_{hh}) = 1 .$$

Näin ollen saadaan

$$\sum_{i=g}^{h}\sum_{j=g}^{h} p(x_i, y_j) = \sum_{i=g}^{h} p(x_i) \underbrace{\leq 1}_{\text{Määritelmä Lf.5}} . \qquad \text{(L1.7)}$$

On osoitettu, että yhteistodennäköisyysjakauma on epätäydellinen. Lisäksi on osoitettu, että lähtöjoukon todennäköisyysjakauman ja yhteistodennäköisyysjauman summat ovat yhtä suuria. ■

3. Lähtöjoukon ja tulojoukon todennäköisyysjakaumien samankaltaisuus

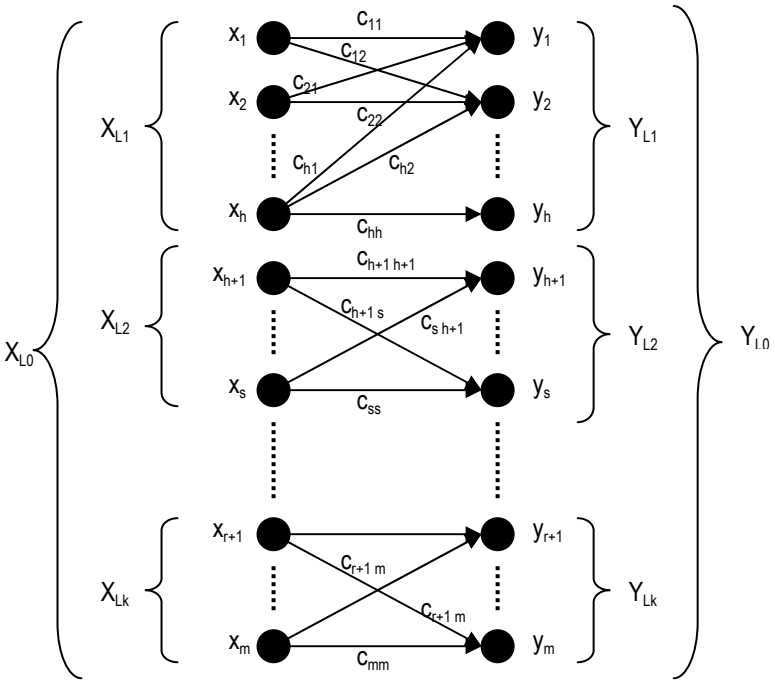
Määritelmä L1.6
Muodostukoon lähtöjoukko emissioympäristön lähettimistä (symboleista) $X = \{x_1, x_2, ..., x_m\}$. Symbolit voidaan edelleen jakaa määritelmän L1.3 mukaisiin lähetekategorioihin $X_{L1}, X_{L2}, ..., X_{Lk} \subset X$. Tulojoukko muodostuu symboleista $Y = \{y_1, y_2, ..., y_m\}$, jotka voidaan myös jakaa määritelmän L1.3 mukaisiin lähetekategorioihin $Y_{L1}, Y_{L2}, ..., Y_{Lk} \subset Y$. Symboleiden kuvautumista säädellään määritelmien L1.1 ja L1.2 mukaisesti. Tällöin siis lähtöjoukon symboli $x_i \in X_{Lt} \subset X$ kuvautuu yhtä suurella todennäköisyydellä kaikiksi samaan lähetekategoriaan kuuluviksi symboleiksi $y_j \in Y_{Lt} \subset Y$, mutta ei voi kuvautua yhdeksikään symboliksi $y_j \notin Y_{Lt}$.

Lause 2: Lähtöjoukon ja tulojoukon todennäköisyysjakaumien samankaltaisuus

Olkoon $X = \{x_1, x_2, ..., x_m\}$ joukko emissioympäristön lähettimiä (symboleita), joita vastaa lähetetodennäköisyysjakauma $P(X_{L0} = x_i) = p(x_i)$, missä i = 1, …, m. Määritelmän L1.6 olosuhteiden vallitessa voidaan todeta, että vastaanottotodennäköisyysjakauma $P(Y_{L0} = y_j) = p(y_j)$ (j = 1, …, m) on täysin sama kuin lähetetodennäköisyysjakauma.

Todistus:

Tilannetta voidaan havainnollistaa alla olevalla kuvalla.



Kuva L1.2: Tilanne, jossa lähetekategoriaan Ln kuuluva symboli x_i voi kuvautua miksi tahansa samaan kategoriaan kuuluvaksi tulojoukon symboliksi y_j. Kuvautumista muihin kategorioihin ei sallita.

Jokaista symbolikategoriajoukkoa X_{Ln} vastaa lähetetodennäköisyysjakauma $P(X_{Ln})$. Muodostetaan näistä jakaumista lähetetodennäköisyysvektorit

$$P_{L1} = (p_1 \quad p_2 \quad \cdots \quad p_h)$$
$$P_{L2} = (p_{h+1} \quad p_{h+2} \quad \cdots \quad p_s)$$
$$\vdots$$
$$P_{Lk} = (p_{r+1} \quad p_{r+2} \quad \cdots \quad p_m)$$

Koska kussakin lähetekategoriajoukossa on vain yhteen ja samaan kategoriaan kuuluvia lähettimiä, ovat yksittäiset todennäköisyydet kategorian sisällä samat, esim. $p_1 = p_2 = \ldots = p_h$. Tämä pätee kaikille jakaumille $P(X_{Ln})$.

Määritelmän L1.6 mukaisesti symboli x_i kuvautuu samalla todennäköisyydellä miksi tahansa samaan kategoriaan kuuluvaksi symboliksi y_j. Kutakin kategoriajoukkoa vastaava kuvautumistodennäköisyysjakauma on näin ollen tasajakauma, jossa yksittäinen kuvautumistodennäköisyys riippuu vain symbolien lukumäärästä. Kaikki kuvautumistodennäköisyydet symbolikategoriajoukon ulkopuolelle ovat nolla. Koska symbolikategoriajoukot sekä lähtö- että tulopuolella ovat itsenäisiä, voidaan kanavamatriisit laatia erikseen niille jokaiselle. Tällöin saadaan

$$C_{L1} = \begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1h} \\ c_{21} & c_{22} & \cdots & c_{2h} \\ \vdots & \vdots & \ddots & \vdots \\ c_{h1} & c_{h2} & \cdots & c_{hh} \end{pmatrix} = \begin{pmatrix} \frac{1}{h} & \frac{1}{h} & \cdots & \frac{1}{h} \\ \frac{1}{h} & \frac{1}{h} & \cdots & \frac{1}{h} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{h} & \frac{1}{h} & \cdots & \frac{1}{h} \end{pmatrix}$$

$$C_{L2} = \begin{pmatrix} c_{h+1h+1} & c_{h+1h+2} & \cdots & c_{h+1s} \\ c_{h+2h+1} & c_{h+1h+2} & \cdots & c_{h+2s} \\ \vdots & \vdots & \ddots & \vdots \\ c_{sh+1} & c_{sh+2} & \cdots & c_{ss} \end{pmatrix} = \begin{pmatrix} \frac{1}{s-h} & \frac{1}{s-h} & \cdots & \frac{1}{s-h} \\ \frac{1}{s-h} & \frac{1}{s-h} & \vdots & \frac{1}{s-h} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{s-h} & \frac{1}{s-h} & \cdots & \frac{1}{s-h} \end{pmatrix}$$

$$C_{Lk} = \begin{pmatrix} c_{r+1r+1} & c_{r+1r+2} & \cdots & c_{r+1m} \\ c_{r+2r+1} & c_{r+2r+2} & \cdots & c_{r+2m} \\ \vdots & \vdots & \ddots & \vdots \\ c_{mr+1} & c_{mr+2} & \cdots & c_{mm} \end{pmatrix} = \begin{pmatrix} \frac{1}{m-r} & \frac{1}{m-r} & \cdots & \frac{1}{m-r} \\ \frac{1}{m-r} & \frac{1}{m-r} & \cdots & \frac{1}{m-r} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{m-r} & \frac{1}{m-r} & \cdots & \frac{1}{m-r} \end{pmatrix}$$

Vastaanottotodennäköisyysvektori saadaan määriteltyä lähetetodennäköisyysvektorin ja kuvautumistodennäköisyysmatriisin tulona

$$V_{Ln} = P_{Ln} C_{Ln} .$$

Tässä $p(y_j) = v_j = \sum_{i=q}^{w} p_i c_{ij}$ ja $j = q, \ldots, w$. Indeksi q merkitsee kunkin kategoriajoukon ensimmäistä alkiota ja indeksi w saman kategorian viimeistä alkiota.

Vastaanottotodennäköisyyksiksi saadaan nyt

$$v_1 = p_1 c_{11} + p_2 c_{21} + \ldots + p_h c_{h1} = \frac{1}{h}\left(p_1 + p_2 + \ldots + p_h\right) = \frac{1}{h} \cdot h p_1 = p_1$$

$$v_2 = p_1 c_{12} + p_2 c_{22} + \ldots + p_h c_{h2} = \frac{1}{h}\left(p_1 + p_2 + \ldots + p_h\right) = \frac{1}{h} \cdot h p_2 = p_2$$

$$\vdots$$

$$v_h = p_1 c_{1h} + p_2 c_{2h} + \ldots + p_h c_{hh} = \frac{1}{h}(p_1 + p_2 + \ldots + p_h) = \frac{1}{h} \cdot h p_h = p_h$$

$$v_{h+1} = p_{h+1} c_{h+1h+1} + \ldots + p_s c_{ss} = \frac{1}{s-h}(p_{h+1} + p_{h+2} + \ldots + p_s) = \frac{1}{s-h} \cdot (s-h) p_{h+1} = p_{h+1}$$

$$\vdots$$

$$\vdots$$

$$v_m = p_{r+1} c_{mr+1} + \ldots + p_m c_{mm} = \frac{1}{m-r}(p_{r+1} + p_{r+2} + \ldots + p_m) = \frac{1}{m-r} \cdot (m-r) p_m = p_m$$

Näin ollen havaitaan

$$V_{L1} = (v_1 \quad v_2 \quad \cdots \quad v_k) = (p_1 \quad p_2 \quad \cdots \quad p_h) = P_{L1}$$
$$V_{L2} = (v_{h+1} \quad v_{h+2} \quad \cdots \quad v_s) = (p_{h+1} \quad p_{h+2} \quad \cdots \quad p_s) = P_{L2}$$
$$\vdots$$
$$V_{Lk} = (v_{r+1} \quad v_{r+2} \quad \cdots \quad v_m) = (p_{r+1} \quad p_{r+2} \quad \cdots \quad p_m) = P_{Lk}$$

ja edelleen siis

$$P(X_{L1}) = P(Y_{L1}) \;\; \forall x_i \in X_{L1} \text{ ja } y_j \in Y_{L1}$$
$$P(X_{L2}) = P(Y_{L2}) \;\; \forall x_i \in X_{L2} \text{ ja } y_j \in Y_{L2}$$
$$\vdots$$
$$P(X_{Lk}) = P(Y_{Lk}) \;\; \forall x_i \in X_{Lk} \text{ ja } y_j \in Y_{Lk}$$

joka johtaa lopputulokseen

$$P(X_{L0}) = P(Y_{L0}) \;\; \forall x_i \in X_{L0} \text{ ja } y_j \in Y_{L0}. \qquad \text{(L1.8)}$$

Lähtöjoukon todennäköisyysjakauma (lähetetodennäköisyysjakauma) on siis täysin sama kuin tulojoukon todennäköisyysjakauma (vastaanottotodennäköisyysjakauma). ■

3. Yhtenäisinformaatio epätäydellisille jakaumille

Eräs tapa ilmaista yhtenäisinformaatio on [16, s. 21] ja [62, s. 21]:

$$I(X;Y) = H(X) + H(Y) - H(X,Y). \qquad \text{(L1.9)}$$

Jos oletetaan, että lähtöjoukon entropiaa $H(X)$ määrittelevä todennäköisyysjakauma on täydellinen, niin tällöin entropia määritetään kaavoilla

$$H(X) = \sum_i p(x_i) \log_2 \frac{1}{p(x_i)} \qquad \text{ja} \qquad H(Y) = \sum_j p(y_j) \log_2 \frac{1}{p(y_j)} \text{ sekä}$$

$$H(X,Y) = \sum_{ij} p(x_i, y_j) \log_2 \frac{1}{p(x_i, y_j)}.$$

Jos lähetetodennäköisyysjakauma on epätäydellinen, niin tällöin lauseessa 1 osoitetun perusteella myös vastaanottotodennäköisyysjakauma ja näiden kahden yhteisjakauma ovat epätäydellisiä ja suuruudeltaan samoja. Rényi on osoittanut [55] (ks. luku 3.2.7), että epätäydellistä jakaumaa vastaava ensimmäisen asteen entropia H_1 voidaan laskea

$$H_1(X) = \frac{\sum_i p(x_i)\log_2 \frac{1}{p(x_i)}}{\sum_i p(x_1)}. \qquad \text{(L1.10)}$$

Tämä määrittely on yhdenmukainen Shannonin entropian kanssa, koska selkeästi $H(X) = H_1(X)$ kun $\sum_i p(x_i) = 1$[55], [56].

Yhtälö L1.9 saadaan nyt siis muotoon

$$I(X;Y) = H_1(X) + H_1(Y) - H_1(X,Y)$$
$$= \frac{\sum_i p(x_i)\log_2 \frac{1}{p(x_i)}}{\sum_i p(x_i)} + \frac{\sum_j p(y_j)\log_2 \frac{1}{p(y_j)}}{\sum_j p(y_j)} - \frac{\sum_{i,j} p(x_i,y_j)\log_2 \frac{1}{p(x_i,y_j)}}{\sum_{i,j} p(x_i,y_j)}. \qquad \text{(L1.11)}$$

Lähtöjoukon painokerroin $W(P_L)$ on määritelty (ks. luku 3.2.7)

$$W(P_L) = \sum_i p(x_i).$$

Lauseen 1 perusteella tiedämme, että

$$W(P_L) = \sum_i p(x_i) = \sum_j p(y_j) = \sum_{i,j} p(x_i,y_j).$$

Yhtälö L1.11 sievenee näin ollen muotoon

$$I(X;Y) = \frac{1}{W(P_L)}\left[\sum_i p(x_i)\log_2 \frac{1}{p(x_i)} + \sum_j p(y_j)\log_2 \frac{1}{p(y_j)} - \sum_{i,j} p(x_i,y_j)\log_2 \frac{1}{p(x_i,y_j)}\right].$$
(L1.12)

Lauseen 2 perusteella tiedämme, että mikäli lähtöjoukon symboli voi kuvautua vain ja ainoastaan samaan symbolikategoriaan kuuluvien symboleiden kanssa ristiin, niin tällöin vastaanottotodennäköisyysjakauma on täysin sama, kuin on lähetetodennäköisyysjakauma (ks. L1.8). Tällöin täytyy myös päteä

$$H_1(X) = H_1(Y). \qquad \text{(L1.13)}$$

Nyt saadaan yhtälö L1.11 muotoon

$$I(X;Y) = 2H_1(X) - H(X,Y). \qquad \text{(L1.14)}$$

Yhtälö L1.12 sievenee edelleen muotoon

$$I(X;Y) = \frac{1}{W(P_L)}\left[2\sum_i p(x_i)\log_2\frac{1}{p(x_i)} - \sum_{i,j} p(x_i,y_j)\log_2\frac{1}{p(x_1,y_j)}\right]. \qquad \text{(L1.15)}$$

4. Yhtenäisinformaation yhteenlaskettavuus

Määritelmä L1.7 – Solujen riippumattomuus
Tämä määritelmä on tarkennus määritelmään L1.1.
Olkoon $X_0 = \{x_1, x_2, \ldots, x_n\}$ joukko symboleita (lähtöjoukko), jotka sijaitsevat rajoitetulla alueella O_0. Oletetaan, että alue O_0 on jaettu soluihin O_1, O_2, …, O_N siten, että $O_1, O_2, ..., O_N \subset O_0$. Lisäksi pätee $\bigcup_{k=1}^{N} O_k = O_0$ ja $\bigcap_{k=1}^{N} O_k = \varnothing$. Oletetaan lisäksi, että symbolit ovat jakautuneet soluihin seuraavasti: $X_1 = \{x_1, \ldots, x_h\}$, $X_2 = \{x_{h+1}, \ldots, x_r\}$, …$X_N = \{x_{s+1}, \ldots, x_n\}$ ja pätee siis $X_1, X_2, ..., X_N \subset X_0$. Tulojoukon Y_0 muodostavat solut $Y_1, Y_2, ..., Y_N \subset Y_0$. Solu on riippumaton muista soluista jos $x_i \in X_r \subset X_0 \mapsto y_j \in Y_s \subset Y_0$ on mahdollista vain silloin, kun $r = s$. Kuvautuminen ei ole mahdollista, jos $r \neq s$. Tällaisessa tilanteessa kuvautumistodennäköisyys c_{rs} on nolla. Tällaiselle kuvatumistodennäköisyydelle käytetään yleismerkintää

$$c_{00} = 0.$$

Määritelmä L1.8
Jatkossa hyödynnetään yhtenäisinformaation määritelmää, joka on muuttujien x_i ja y_j yhteistodennäköisyysjakauman sekä näiden marginaalitodennäköisyysjakaumien tulon välinen suhteellinen entropia (ks. luku 3.2.8 yhtälöt 3.20 ja 3.21).

Suhteellisen entropian määritelmälle ovat voimassa tulkinnat (ks. [16, s. 19])

$$0\log_2\frac{0}{0} = 0, \qquad 0\log_2\frac{0}{q} = 0 \text{ ja} \qquad p\log_2\frac{p}{0} = \infty.$$

<u>Lause 3: Yhtenäisinformaation yhteenlaskettavuus</u>
Solujen ollessa toisistaan riippumattomia määritelmän L1.7 mukaisesti, koko alueen yhtenäisinformaatio on erillisten solujen yhteisinformaatioiden summa eli

$$I(X_0;Y_0) = I(X_1;Y_1) + I(X_2;Y_2) + ... + I(X_N;Y_N). \qquad \text{(L1.16)}$$

<u>Todistus:</u>

Lasketaan yhtenäisinformaatiot kullekin solulle erikseen. Lähtemällä liikkeelle luvussa 3.2.8 esitellystä yhtälöstä 3.21 saadaan

$$I(X_1;Y_1) = \sum_{i=1}^{h}\sum_{j=1}^{h} p(x_i,y_j)\log_2\frac{p(x_i,y_j)}{p(x_i)p(y_j)} = \underbrace{p(x_1,y_1)\log_2\frac{p(x_1,y_1)}{p(x_1)p(y_1)}}_{w11} + ...$$

$$+ \underbrace{p(x_1,y_h)\log_2\frac{p(x_1,y_h)}{p(x_1)p(y_h)}}_{w1h} + \underbrace{p(x_2,y_1)\log_2\frac{p(x_2,y_1)}{p(x_2)p(y_1)}}_{w21} + ...$$

$$+ \underbrace{p(x_h, y_h)\log_2 \frac{p(x_h, y_h)}{p(x_h)\,p(y_h)}}_{whh}$$

$$= w_{1,1} + w_{1,2} + \ldots + w_{1,h} + w_{2,1} + \ldots + w_{h,h} = \sum_{i=1}^{h}\sum_{j=1}^{h} w_{i,j} \ . \quad \text{(L1.17)}$$

Korvaamalla logaritmilausekkeet yllä esitetyllä logiikalla, saadaan muille soluille yhtenäisinformaatiot

$$I(X_2;Y_2) = w_{h+1,h+1} + w_{h+1,h+2} + \ldots + w_{h+2,h+1} + \ldots + w_{r,h+1} + \ldots + w_{r,r} = \sum_{i=h+1}^{r}\sum_{j=h+1}^{r} w_{i,j}$$

$$\vdots$$

$$I(X_N;Y_N) = w_{s+1,s+1} + w_{s+1,s+2} + \ldots + w_{s+2,s+1} + \ldots + w_{n,s+1} + \ldots + w_{n,n} = \sum_{i=s+1}^{n}\sum_{j=s+1}^{n} w_{i,j}$$

Lasketaan yhteen eri solujen yhtenäisinformaatiot:

$$\sum_{k=1}^{N} I(X_k;Y_k) = \sum_{i=1}^{h}\sum_{j=1}^{h} w_{i,j} + \sum_{i=h+1}^{r}\sum_{j=h+1}^{r} w_{i,j} + \ldots + \sum_{i=s+1}^{n}\sum_{j=s+1}^{n} w_{i,j} \ . \quad \text{(L1.18)}$$

Lasketaan seuraavaksi yhtenäisinformaatio koko joukolle X_0.

$$\begin{aligned} I(X_0;Y_0) &= w_{1,1} + \ldots + w_{1,h} + w_{1,h+1} + \ldots + w_{1,r} + \ldots + w_{1,n} + \ldots \\ &+ w_{2,1} + \ldots + w_{2,h} + \ldots + w_{2,r} + \ldots + w_{2,n} + \ldots\ldots + w_{n,1} + \ldots + w_{n,n} \end{aligned} \quad \text{(L1.19)}$$

Irrotetaan yllä olevasta yhtälöstä summa

$$w_{1,1} + w_{1,2} + \ldots + w_{1,h} + w_{1,h+1} + \ldots + w_{1,r} + \ldots + w_{1,n} = \sum_{j=1}^{n} w_{1,j} \ . \quad \text{(L1.20)}$$

Havaitaan, että summa L1.20 sisältää lausekkeita, jotka eivät esiinny summassa L1.18 (esimerkiksi $w_{1,h+1}$ ja $w_{1,n}$). Summien eron suuruus saadaan selville vähentämällä molemmille summille yhteiset osat lausekkeesta L1.20. Tällöin saadaan

$$\sum_{j=1}^{n} w_{1,j} - \sum_{j=1}^{h} w_{1,j} = \sum_{j=h+1}^{n} w_{1,j} \ . \quad \text{(L1.21)}$$

Erotuksen jälkeen jäljelle jäänyt osa on toisin kirjattuna

$$\sum_{j=h+1}^{n} p(x_1, y_j)\log_2 \frac{p(x_1, y_j)}{p(x_1)\,p(y_j)} = p(x_1, y_{h+1})\log_2 \frac{p(x_1, y_{h+1})}{p(x_1)\,p(y_{h+1})} + \ldots + p(x_1, y_n)\log_2 \frac{p(x_1, y_n)}{p(x_1)\,p(y_n)}$$

(L1.22)

Kuten havaitaan, pyritään symboli $x_1 \in X_1 \mapsto y_{h+1} \notin Y_1$, eli symboli x_1 pyritään kuvaamaan joukkoon, joka ei vastaa solun tulojoukkoa. Näin on tilanne kaikkien yhtälössä L1.22 esiintyvien yhdistelmien x_1 ja y_j suhteen. Määritelmän L1.7 mukaisesti tällöin kuvautumistodennäköisyys on $c_{00} = 0$. Tiedetään, että

$$p(x_i, y_j) = p(x_i)\,p(y_j \mid x_i) = p(x_i)c_{ij} = 0, \text{ jos } c_{ij} = c_{00} = 0. \qquad \text{(L1.23)}$$

Soveltamalla määritelmää L1.8 lopputulokseksi saadaan tilanne, jossa kaikille yhtälön L1.22 logaritmilausekkeille pätee

$$p(x_1, y_j)\log_2 \frac{p(x_1, y_j)}{p(x_1)\,p(y_j)} = 0 \log_2 \frac{0}{p(x_1)\,p(y_j)} = 0 \quad \forall\ j \in \{h+1, \ldots, n\}. \qquad \text{(L1.24)}$$

Nyt saadaan yhtälön L1.21 lopputulokseksi

$$\sum_{j=1}^{n} w_{1,j} - \sum_{j=1}^{h} w_{1,j} = \sum_{j=h+1}^{n} w_{1,j} = 0\,. \qquad \text{(L1.25)}$$

Lausekkeen L1.24 mukainen lopputulos saadaan aikaiseksi kaikille sellaisille x_i ja y_j yhdistelmille, joille määritelmän L1.7 mukaisesti kuvautumistodennäköisyydeksi tulee $c_{00} = 0$. Edelleen päädytään yhtälön L1.25 mukaiseen lopputulokseen, kun vaiheet L1.20 ja L1.21 toistetaan kaikille *i* ja *j*. Käytännössä siis toteutetaan vähennyslasku L1.26 ja todetaan, että tulos on nolla.

$$I(X_0; Y_0) - \sum_{k=1}^{N} I(X_k; Y_k) = 0 \qquad \text{(L1.26)}$$

Tämä tarkoittaa, että summat L1.18 ja L1.19 ovat yhtä suuria eli

$$I(X_0; Y_0) = I(X_1; Y_1) + I(X_2; Y_2) + \ldots + I(X_N; Y_N)\,. \qquad \text{(L1.27)}$$ ■

5. Epätäydellisen tasajakauman entropia

Olkoon $X = \{x_1, x_2, \ldots, x_n\}$ joukko symboleita, joiden yleisyyttä kuvaa diskreetti todennäköisyysjakauma $P(X=x_i)=p(x_i)$, $i = 1, 2, \ldots, n$. Jakauma on tasajakauma eli $p_1 = p_2 = \ldots = p_n = P_L$. Lisäksi oletetaan, että jakauma on epätäydellinen.

Lause 4: Epätäydellisen tasajakauman entropia
Ensimmäisen asteen entropia on tällöin:

$$H_1(X) = \log_2 \frac{1}{P_L} \qquad \text{(L1.28)}$$

Todistus:

Lähtemällä liikkeelle ensimmäisen asteen entropian määrittelystä epätäydelliselle jakaumalle [55] saadaan

$$H_1(X) = \frac{\sum_{i=1}^{n} p(x_i) \log_2 \frac{1}{p_i}}{\sum_{i=1}^{n} p(x_i)} = \frac{nP_L \log_2 \frac{1}{P_L}}{nP_L} = \log_2 \frac{1}{P_L}. \qquad \text{(L1.29)}$$

■

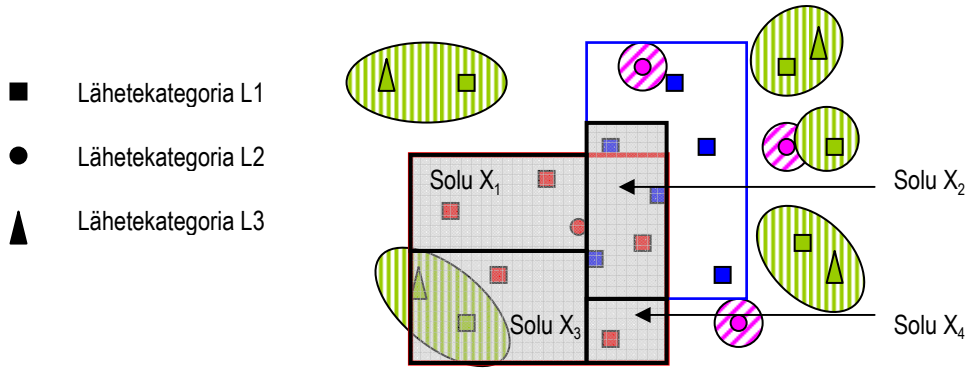
ESIMERKKI KRIITTISEN TOIMINNAN TUNNISTAMISESTA

Olkoon tarkasteltava tilanne kuvan L2.1 mukainen. Oletetaan, että lähetekategoriaa L1 vastaa lähetetodennäköisyys P_{L1} = 0.0159, kategoriaa L2 vastaa P_{L2} = 0.1667 ja kategoriaa L3 vastaa P_{L3} = 0.0833. Lähetetodennäköisyydet ovat esimerkin 4.1 mukaiset. Lähettimet ovat jakautuneet soluihin seuraavasti:

$$X_1 = \left\{x_1^{L1}, x_2^{L1}, x_3^{L2}\right\}$$
$$X_2 = \left\{x_4^{L1}, x_5^{L1}, x_6^{L1}, x_7^{L1}\right\}$$
$$X_3 = \left\{x_8^{L1}, x_9^{L1}, x_{10}^{L3}\right\}$$
$$X_4 = \left\{x_{11}^{L1}\right\}$$

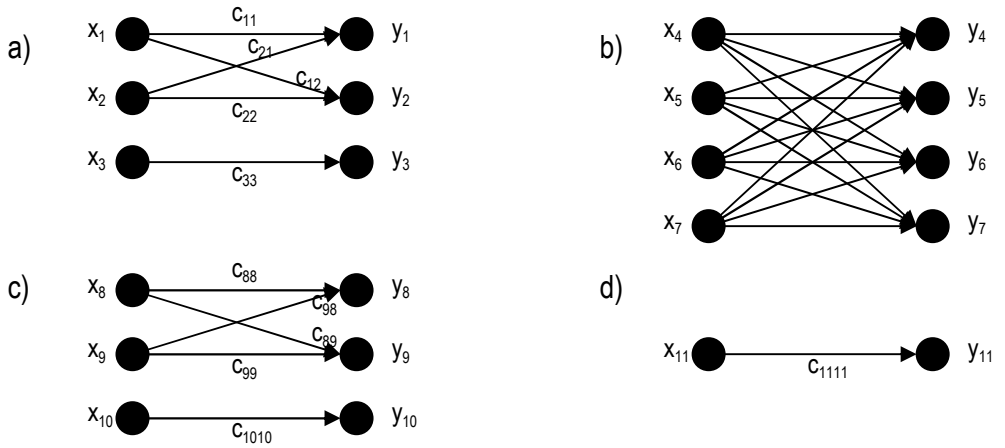
Näin ollen saadaan lähetetodennäköisyysvektorit:

$$P_{X1} = \left(p_1 \quad p_2 \quad p_2\right) = \left(0.0159 \quad 0.0159 \quad 0.1667\right)$$
$$P_{X2} = \left(p_4 \quad p_5 \quad p_6 \quad p_7\right) = \left(0.0159 \quad 0.0159 \quad 0.0159 \quad 0.0159\right)$$
$$P_{X3} = \left(p_8 \quad p_9 \quad p_{10}\right) = \left(0.0159 \quad 0.0159 \quad 0.0833\right)$$
$$p_{11} = 0.0159$$



Kuva L2.1: Esimerkki, jossa tarkastelun kohteena punaisella merkitty kriittinen toiminta / osajoukko (X_0). Alue jaettu tarkastelua varten neljään pienempää soluun (X_1, X_2, X_3 ja X_4).

Jokaisen solun kohdalla tarkastellaan, miten samaan lähetekategoriaan kuuluvan lähettimet voivat kuvautua ristiin. Lähettimet eivät saa kuvautua solunsa ulkopuolelle. Solujen kuvautumista on havainnollistettu kuvissa L2.2 a, b, c, d.



Kuva L2.2: Kuvautuminen eri soluissa. a) Solu X_1 b) Solu X_2 c) Solu X_3 d) Solu X_4

Liitteessä 1 on osoitettu, että tällaisissa tilanteissa lähetetodennäköisyysjakauma on aina sama, kuin on vastaanottotodennäköisyysjakauma. Näin ollen saadaan suoraan vastaanottotodennäköisyysvektorit:

$$V_{X1} = P_{X1} = (v_1 \quad v_2 \quad v_3) = (0.0159 \quad 0.0159 \quad 0.1667)$$
$$V_{X2} = P_{X2} = (v_4 \quad v_5 \quad v_6 \quad v_7) = (0.0159 \quad 0.0159 \quad 0.0159 \quad 0.0159)$$
$$V_{X3} = P_{X3} = (v_8 \quad v_9 \quad v_{10}) = (0.0159 \quad 0.0159 \quad 0.0833)$$
$$v_{11} = p_{11} = 0.0159$$

Kuvautumistodennäköisyydet eri soluissa ovat:

$$C_1 = \begin{pmatrix} c_{11} & c_{12} & c_{13} \\ c_{21} & c_{22} & c_{23} \\ c_{31} & c_{32} & c_{33} \end{pmatrix} = \begin{pmatrix} 0.5 & 0.5 & 0 \\ 0.5 & 0.5 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$C_2 = \begin{pmatrix} c_{44} & c_{45} & c_{46} & c_{47} \\ c_{54} & c_{55} & c_{56} & c_{57} \\ c_{64} & c_{65} & c_{66} & c_{67} \\ c_{74} & c_{75} & c_{76} & c_{77} \end{pmatrix} = \begin{pmatrix} 0.25 & 0.25 & 0.25 & 0.25 \\ 0.25 & 0.25 & 0.25 & 0.25 \\ 0.25 & 0.25 & 0.25 & 0.25 \\ 0.25 & 0.25 & 0.25 & 0.25 \end{pmatrix}$$

$$C_3 = \begin{pmatrix} c_{88} & c_{89} & c_{810} \\ c_{98} & c_{99} & c_{910} \\ c_{108} & c_{109} & c_{1010} \end{pmatrix} = \begin{pmatrix} 0.5 & 0.5 & 0 \\ 0.5 & 0.5 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$c_{1111} = 1$$

Lasketaan yhteistodennäköisyysjakauma $P(X,Y)$, joka saadaan

$$p(x_i, y_j) = p(x_i)\,p(y_j \mid x_i) = p_i c_{ij}\,.$$

Solu 1:

	x1	**x2**	**x3**		
y1	$p_1 c_{11}$ $= 0.00795$	$p_2 c_{21}$ $= 0.00795$	0		
y2	$p_1 c_{12}$ $= 0.00795$	$p_2 c_{22}$ $= 0.00795$	0		
y3	0	0	$p_3 c_{33}$ $= 0.1667$		

Solu 2:

	x4	**x5**	**x6**	**x7**	
y4	p_4c_{44} = 0.00398	p_5c_{54} = 0.00398	p_6c_{64} = 0.00398	p_7c_{74} = 0.00398	
y5	p_4c_{45} = 0.00398	p_5c_{55} = 0.00398	p_6c_{65} = 0.00398	p_7c_{75} = 0.00398	
y6	p_4c_{46} = 0.00398	p_5c_{56} = 0.00398	p_6c_{66} = 0.00398	p_7c_{76} = 0.00398	
y7	p_4c_{47} = 0.00398	p_5c_{57} = 0.00398	p_6c_{67} = 0.00398	p_7c_{77} = 0.00398	

Solu 3:

	x8	**x9**	**x10**		
y8	p_8c_{88} = 0.00795	p_9c_{98} = 0.00795	0		
y9	p_8c_{89} = 0.00795	p_9c_{99} = 0.00795	0		
y10	0	0	$p_{10}c_{1010}$ = 0.0833		

Solu 4:

$$p_{11}c_{1111} = 0.0159$$

Lasketaan yhtenäisinformaatio jokaiselle solulle erikseen yhtälöllä

$$I(X;Y) = \frac{1}{W(P_L)}\left[2\sum_i p(x_i)\log_2\frac{1}{p(x_i)} - \sum_{i,j} p(x_i,y_j)\log_2\frac{1}{p(x_1,y_j)}\right].$$

Solu 1:

$$W(P_L) = 2\cdot 0.0159 + 0.1667 = 0.1985$$

$$I_1(X_1;Y_1) = \frac{1}{0.1985}\left\{4\cdot 0.0159\log_2\frac{1}{0.0159} + 2\cdot 0.1667\log_2\frac{1}{0.1667} - \left[4\cdot 0.00795\log_2\frac{1}{0.00795}\right.\right.$$

$$\left.\left. + 0.1667\log_2\frac{1}{0.1667}\right]\right\} = 2.96758bit \approx 2.9676bit$$

Solu 2:

$$W(P_L) = 4\cdot 0.0159 = 0.0636$$

$$I_2(X_2;Y_2) = \frac{1}{0.0636}\left\{8\cdot 0.0159\log_2\frac{1}{0.0159} - 16\cdot 0.00398\log_2\frac{1}{0.00398}\right\}$$

$$= 3.96662bit \approx 3.9666bit$$

Solu 3:

$$W(P_L) = 2 \cdot 0.0159 + 0.0833 = 0.1151$$

$$I_3(X_3;Y_3) = \frac{1}{0.1151}\left\{4 \cdot 0.0159 \log_2 \frac{1}{0.0159} + 2 \cdot 0.0833 \log_2 \frac{1}{0.0833} - \left[4 \cdot 0.00795 \log_2 \frac{1}{0.00795}\right.\right.$$

$$\left.\left. + 0.0833 \log_2 \frac{1}{0.0833}\right]\right\} = 3.96937 bit \approx 3.9694 bit$$

Solu 4:

$$W(P_L) = 0.0159$$

$$I_4(X_4;Y_4) = \frac{1}{0.0159}\left\{2 \cdot 0.0159 \log_2 \frac{1}{0.0159} - 0.0159 \log_2 \frac{1}{0.0159}\right\}$$

$$= \frac{1}{0.0159}\left(0.0159 \log_2 \frac{1}{0.0159}\right) = \log_2 \frac{1}{0.0159} = 5.97483 bit \approx 5.9748 bit$$

Kuten liitteessä 1 on osoitettu, voidaan koko alueen yhtenäisinformaatio laskea solujen informaatioiden summana

$$I(X_0;Y_0) = \sum_{k=1}^{4} I_k(X_k;Y_k) = 2.96758 bit + 3.96662 bit + 3.96937 bit + 5.97483 bit$$

$$= 16.8784 bit$$

Miten saatuun yhtenäisinformaatioon tulisi suhtautua? Tämän selvittämiseksi on laskettava alueen (ja solujen) alkuperäinen entropia ja verrattava yhteisinformaatiota tähän.

Solujen entropiat lasketaan luvussa 3.2.7 esitellyn yhtälön 3.16 mukaisesti:

$H_1(X_1) = 3.12778 bit \approx 3.1278 bit$

$H_1(X_2) = 5.97483 bit \approx 5.9748 bit$

$H_1(X_3) = 4.24565 bit \approx 4.2457 bit$

$H_1(X_4) = 5.97483 bit \approx 5.9748 bit$

Koko alueen entropia saadaan näiden summana

$$H_1(X_0) = \sum_{k=1}^{4} H_1(X_k) = 19.32309 bit \approx 19.3231 bit .$$

Entropiaa ja yhtenäisinformaatiota voidaan vertailla keskenään solu- ja aluekohtaisesti. Tällöin saadaan seuraavia tuloksia.

	Entropia H	Yhtenäisin-formaatio I	Erotus (H-I)	Prosenttia I/H
Solu 1	3.1278	2.9676	0.1602	94.9 %
Solu 2	5.9748	3.9666	2.0082	66.4 %
Solu 3	4.2457	3.9694	0.2763	93.5 %
Solu 4	5.9748	5.9748	0	100 %
Koko alue	19.3231	16.8784	2.4447	87.3 %

Tuloksia tulkitaan siten, että mitä pienempi on entropian ja yhteisinformaation erotus (ehdollinen entropia), niin sitä helpompi tällaiselta alueelta erottuvat kriittisen toiminnan tai tarkasteltavan osajoukon lähettimet. Prosenttiosuus kertoo yhtenäisinformaation suhteellisen osuuden solun tai alueen entropiasta. Prosenttiosuus voidaan mieltää varmuudeksi (todennäköisyydeksi), jolla solun tai alueen lähettimet kyetään yksilöimään vain tuntemalla niiden lähetekategoria. Tässä esimerkissä solu 2 on ”epäselvin” ja symboleiden mahdollinen kuvautuminen ristiin aiheuttaa sen, että lähetinten yksilöinti juuri tietyksi lähettimeksi on mahdollista vain noin 66 prosentin varmuudella. Solun numero 4 lähetin kyetään yksilöimään 100 % varmuudella, koska solussa ei ole yhtään kuvautumista sekoittavaa lähetintä.

ESIMERKKI 4.5 – EMISSIOMALLIEN ENTROPIA

1. Emissiomallien entropiat

Osajoukko A

Osajoukko A sisältää symbolit $A = \{a_1, a_2, a_3, a_4, a_5\}$, joita vastaa todennäköisyysjakauma $P(A=a_i) = p(a_i) = (0.143, 0.143, 0.143, 0.143, 0.428)$. Emissiomalli on luvun 4.3.1 kuvassa 4.7 esitetynlainen. Peräkkäisten symbolien esiintyminen on näin ollen toisistaan riippumatonta. Tällöin emissiomallin entropia voidaan laskea luvun 4.3.2 yhtälön 4.19 mukaisesti

$$H_s(A) = \sum_{i=1}^{5} p(a_i)\log_2\frac{1}{p(a_i)} = 4\times\left(0.143\log_2\frac{1}{0.143}\right) + 0.428\log_2\frac{1}{0.428} = 2.128990\,\frac{bit}{symboli}$$

$$\approx 2.13\,\frac{bit}{symboli}.$$

Mikä olisi tämän ympäristön suurin mahdollinen entropia? Saadaan yhtälöllä 4.18

$$H_{sU}(A) = \log_2 5 = 2.321928\,\frac{bit}{symboli} \approx 2.32\,\frac{bit}{symboli}.$$

Osajoukko D

Osajoukko D sisältää symbolit $D = \{d_1, d_2, d_3, d_4\}$. Emissiomalli on luvun 4.3.1 kuvan 4.8 mukainen eli peräkkäisten symbolien esiintymistä säädellään siirtymätodennäköisyyksillä. Oletetaan, että siirtymätodennäköisyydet ovat

$$P = \begin{pmatrix} P_{11} & P_{12} & P_{13} & P_{14} \\ P_{21} & P_{22} & P_{23} & P_{24} \\ P_{31} & P_{32} & P_{33} & P_{34} \\ P_{41} & P_{42} & P_{43} & P_{44} \end{pmatrix} = \begin{pmatrix} 0.3 & 0.5 & 0.2 & 0 \\ 0.2 & 0.6 & 0.2 & 0 \\ 0.5 & 0 & 0 & 0.5 \\ 0.2 & 0 & 0.2 & 0.6 \end{pmatrix}.$$

Entropian laskemiseksi tarvitaan ensin rajatodennäköisyydet μ_i. Hyödyntämällä luvussa 3.3.1 esitettyjä yhtälöitä 3.31 ja 3.32 saadaan muodostettua seuraavanlainen yhtälöryhmä:

$$\mu_1 = 0.3\mu_1 + 0.2\mu_2 + 0.5\mu_3 + 0.2\mu_4$$
$$\mu_2 = 0.5\mu_1 + 0.6\mu_2 + 0 + 0$$
$$\mu_3 = 0.2\mu_1 + 0.2\mu_2 + 0 + 0.2\mu_4$$
$$\mu_4 = 0 + 0 + 0.5\mu_3 + 0.6\mu_4$$

ja $\mu_1 + \mu_2 + \mu_3 + \mu_4 = 1$

Yhtälöryhmän perusteella saadut rajatodennäköisyydet esitetty alla olevassa vektorissa:

$$\mu = \begin{pmatrix} \mu_1 & \mu_2 & \mu_3 & \mu_4 \end{pmatrix} \approx \begin{pmatrix} 0.28 & 0.35 & 0.17 & 0.21 \end{pmatrix}.$$

Entropia voidaan nyt laskea

$$H_s(D) = \sum_{\substack{i=1 \\ j=1}}^{4} \mu_i P_{ij} \log_2 \frac{1}{P_{ij}} = 0.28\left(0.3\log_2 \frac{1}{0.3} + 0.5\log_2 \frac{1}{0.5} + 0.2\log_2 \frac{1}{0.2} + 0 \right)$$

$$+ 0.35\left(0.2\log_2 \frac{1}{0.2} + 0.6\log_2 \frac{1}{0.6} + 0.2\log_2 \frac{1}{0.2} + 0 \right) + 0.17\left(0.5\log_2 \frac{1}{0.5} + 0 + 0 + 0.5\log_2 \frac{1}{0.5} \right)$$

$$+ 0.21\left(0.2\log_2 \frac{1}{0.2} + 0 + 0.2\log_2 \frac{1}{0.2} + 0.6\log_2 \frac{1}{0.6} \right) = 1.354483 \frac{bit}{symboli} \approx 1.35 \frac{bit}{symboli}$$

Osajoukon D suurin mahdollinen entropia on

$$H_{sU}(D) = \log_2 4 = 2.0 \frac{bit}{symboli}.$$

Osajoukko F

Osajoukko F muodostuu kuvan 4.9 mukaisesta radiolinkkiverkosta. Yhtä linkkijännettä mallinnetaan kuvan 4.10 b mukaisella Markov ketjulla. Malli sisältää symboli $F = \{f_1, f_2\}$. Siirtymätodennäköisyydet *Pij* alla olevan matriisin mukaisesti

$$P = \begin{pmatrix} P_{11} & P_{12} \\ P_{21} & P_{22} \end{pmatrix} = \begin{pmatrix} 0.1 & 0.9 \\ 0.9 & 0.1 \end{pmatrix}.$$

Rajatodennäköisyydet ovat: $\mu_i = [\mu_1 \quad \mu_2] = [0.5 \quad 0.5]$, joka tarkoittaa, että joka toinen symboli on lähtöisin tilasta f_1 ja joka toinen tilasta f_2. Tämä tilanne on linkkijänteen mallinnukselle paras mahdollinen. Linkkijänteen entropia on

$$H_s(F) = \sum_{\substack{i=1 \\ j=1}}^{2} \mu_i P_{ij} \log_2 \frac{1}{P_{ij}} = 0.5\left(0.1\log_2 \frac{1}{0.1} + 0.9\log_2 \frac{1}{0.9} \right) + 0.5\left(0.9\log_2 \frac{1}{0.9} + 0.1\log_2 \frac{1}{0.1} \right)$$

$$= 0.468996 \frac{bit}{symboli} \approx 0.47 \frac{bit}{symboli}.$$

Jos kaikkien neljän linkkijänteen prosessit oletetaan toisistaan riippumattomiksi, saadaan koko verkon entropiaksi 4 x 0.47 = 1.88 bit/symboli.

2. Entropian nopeus

Osajoukko A

Oletetaan, että osajoukkoa A kuvaavan emissiomallin symbolinopeus on φ = 0.5 symbolia/sekunti (malli tuottaa symbolin aina kahden sekunnin välein). Lasketaan osajoukon keskimääräinen entropian nopeus (vrt. luku 4.3.2 yhtälö 4.21):

$$H_s'(A) = \varphi \cdot H_s(A) = 0.5 \frac{symbolia}{s} \cdot 2.1290 \frac{bit}{symboli} = 1.064495 \frac{bit}{s} \approx 1.06 \frac{bit}{s}.$$

Osajoukko D

Oletetaan, että osajoukolla D on seuraavat kutakin tilaa vastaavat symbolinopeudet:

$$\varphi = \begin{pmatrix} \varphi_1 \\ \varphi_2 \\ \varphi_3 \\ \varphi_4 \end{pmatrix} = \begin{pmatrix} 0.2 \\ 0.1 \\ 0.05 \\ 0.2 \end{pmatrix}$$

Keskimääräinen symbolinopeus on $\varphi_{avg} = \frac{\sum_{i=1}^{4} \varphi_i}{4} = 0.14 \frac{symboli}{s}$. Entropian nopeudeksi saadaan nyt (vrt. luku 4.3.2 yhtälö 4.22)

$$H_s^{'}(D) = \varphi_{avg} H_s(D) = 0.14 \cdot 1.35 \approx 0.19 \frac{bit}{s}.$$

Osajoukko F

Osajoukon F osalta on edellä mainittu, että radiolinkki lähettää jatkuvasti ja näin ollen joko symbolin pituuden tai symbolinopeuden tulisi olla ääretön. Käytännön mallinnuksessa symbolinopeus on kuitenkin asetettava äärelliseksi luvuksi. Asetetaan tässä esimerkissä kummankin prosessin tilan symbolinopeus olemaan $\varphi_1 = \varphi_2 = 1000$ symbolia/sek (ks. perustelu alla). Lasketaan yksittäisen linkkijänteen intensiteetti ja koko verkon entropian intensiteetti.

$$H_s^{'}(F) = \varphi_{avg} H_s(F) = 1000 \cdot 0.47 = 470 \frac{bit}{s}$$

Neljän linkkijänteen intensiteetti on näin ollen 1880 bit/s.

Jonkin symbolinopeuden asettaminen kuvaamaan jatkuvasti lähettävien radiolinkkien aktiivisuutta on varsin keinotekoinen ja kaksitahoinen ratkaisu. Symbolinopeuden tulee riittävässä määrin kuvata lähetteen jatkuvaa luonnetta, kun taas toisaalta hyvin suureksi asetettu symbolinopeus saattaa liiaksi korostaa linkkijänteiden intensiteettiä suhteessa muihin osajoukkohin. Yllä linkkijännettä kuvaavan prosessin tiloille annettiin symbolinopeuden arvoksi 1000 symbolia/sek, joka on melko kaukana äärettömästä. Valintaa on perusteltu seuraavassa.

Jos oletetaan, että radiolinkki toimii jossain VHF/UHF taajuusalueella ja se pyritään havaitsemaan sekä suuntimaan tyypillisellä nykyaikaisella viestitiedustelujärjestelmällä, niin hyvin karkeasti arvioiden radiolinkin taajuudella käydään kerran sekunnissa. Tämä perustuu siihen, että tyypillinen VHF/UHF taajuusalueen viestitiedustelujärjestelmä toimii taajuusalueella 20 MHz – 3 GHz, pyyhkäisynopeus on luokkaa 2 – 3 GHz/s ja kohteen suuntiminen edellyttää pysymistä taajuudella vähintään 1 ms ajan [18], [21] ja [69]. Näin ollen, ilman yksityiskohtaisempia analyyseja ja teoreettisesti, tiedusteluvastaanotin käy linkin taajuudella noin sekunnin välein. Jos vielä mielletään, että tuotetun symboli pituus on hyvin lähellä 1 ms:a (joka siis tarvitaan, jotta signaali olisi suunnittavissa), niin tällöin symbolinopeus 1000 symbolia/sekunti tuottaa lähes jatkuvaa lähetettä vastaavan tilanteen.

EHDOLLINEN ENTROPIA JA ESIMERKKI TIEDUSTELUJÄRJESTELMÄN SUHTEELLISEN KAPASITEETIN MÄÄRITTÄMISESTÄ

Liitteessä on kaksi osiota. Ensimmäisessä osoitetaan, että ehdollinen entropia voidaan määrittää vain häiriöiden takia vastaanottamatta jääneiden symbolien avulla. Toisessa osiossa on laskettu esimerkki tiedustelujärjestelmän suhteellisen kapasiteetin määrittämisestä.

1. Ehdollisen entropian määrittäminen

Määritelmä L4.1
Olkoon $X = \{x_1, x_2, ..., x_n\}$joukko symboleita, joiden esiintymistä informaation lähteessä kuvataan diskreetillä todennäköisyysjakaumalla $P(X=x_i) = p(x_i) = p_i$, $i = 1, \ldots, n$. Olkoon lisäksi $Y = \{y_1, y_2, ..., y_n, y_{n+1}\}$joukko symboleita, joiksi lähteen tuottamat symbolit kuvautuvat ja diskreetti todennäköisyysjakauma $P(Y = y_j) = p(y_j) = v_j$ ($j = 1, \ldots, n+1$) kuvatkoon vastaanotettujen symbolien jakaumaa. Lähetettäessä mikä tahansa symboli $x_k \in X$ kohinallisen kanavan yli, se kuvautuu itseään vastaavaksi symboliksi $y_k \in Y$ todennäköisyydellä c_{kk} tai symboliksi $y_{n+1} \in Y$ (merk. $y_{n+1} = S$) todennäköisyydellä $c_{kn+1} = 1 - c_{kk}$. Symboli x_k ei voi kuvautua miksikään muuksi joukkoon Y kuuluvista symboleista. Symboli x_k ei myöskään voi kuvautua joukon Y ulkopuolelle, eikä joukkoon Y voi kuvautua symboleita joukon X ulkopuolelta.

Huomautus L4.1
Jatkossa huomioitava, että logaritmille pätee seuraava (ks. esim. [4, s. 291]:

$-p \log_2 p = 0$, kun $p = 0$.

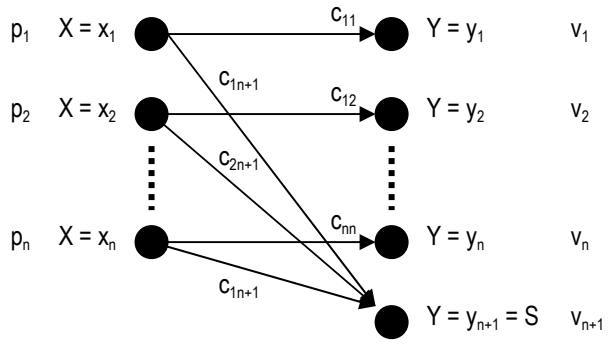
Lisäksi tiedetään, että

$\log_2 p = 0$, kun $p = 1$.

Lause 5: Ehdollisen entropian määrittäminen
Määritelmän L4.1 mukaisten olosuhteiden vallitessa, ehdollinen entropia $H(X|Y)$ voidaan määrittää

$$H(X \mid Y) = \sum_{i=1}^{n} p(x_i, y = S) \log \frac{1}{p(x_i \mid y = S)}. \qquad \text{(L4.1)}$$

Todistus:
Kanava voidaan havainnollistaa kuvan L4.1 mukaisesti.



Kuva L4.1: Symbolien kuvautuminen häiriöllisen kanavan yli.

Lähteen symboleita vastaava todennäköisyysvektori olkoon

$$P_X = (p_1 \quad p_2 \quad \cdots \quad p_n).$$

Symboleiden kuvautumista lähteestä kanavan yli vastaanottimelle kuvaa kanavamatriisi **C**, jossa alkio c_{ij} kuvaa symbolin x_i kuvautumista symboliksi y_j. Määritelmän L4.1 mukaisten kuvautumisvaatimusten johdosta lopputuloksena on matriisi, jossa vain alkioilla c_{ij}, kun $i = j$, ja sarakevektorilla c_{in+1} (missä $i = 1, 2, \ldots, n$) on nollasta poikkeavat arvot. Loput matriisin alkiot ovat nollia. Kanavamatriisiksi saadaan siis

$$C = \begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n} & c_{1n+1} \\ c_{21} & c_{22} & \cdots & c_{2n} & c_{2n+1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ c_{n1} & c_{n2} & \cdots & c_{nn} & c_{nn+1} \end{pmatrix} = \begin{pmatrix} c_{11} & 0 & 0 & \cdots & c_{1n+1} \\ 0 & c_{22} & 0 & \cdots & c_{2n+1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & c_{nn} & c_{nn+1} \end{pmatrix}. \qquad \text{(L4.2)}$$

Voidaan laskea vastaanottotodennäköisyydet $P(Y=y_j) = v_j$ vektorin $\mathbf{P_X}$ ja matriisin **C** tulona:

$$v = P_X C = (v_1 \quad v_2 \quad \cdots \quad v_{n+1}), \qquad \text{missä } v_j = \sum_{i=1}^{n} p_i c_{ij} \text{ ja } j = 1, 2, \ldots, n+1.$$

Johtuen matriisin **C** rakenteesta, saadaan v_j määritettyä varsin yksinkertaisesti:

$$\begin{aligned} v_1 &= p_1 c_{11} \\ v_2 &= p_2 c_{22} \\ &\vdots \\ v_n &= p_n c_{nn} \\ v_{n+1} &= p_1 c_{1n+1} + p_2 c_{2n+1} + \cdots + p_n c_{nn+1} \end{aligned} \qquad . \qquad \text{(L4.3)}$$

X:n ja Y:n yhteinen todennäköisyysjakauma määritetään

$$p(x_i, y_j) = p(x_i)\, p(y_j \mid x_i) = p_i c_{ij}\,.$$

Edellä todettiin, että c_{ij} saa nollasta poikkeavia arvoja vain, kun $i = j$ ja kun $j = n+1$. Näin ollen yhteiseksi todennäköisyysjakaumaksi saadaan:

	$\mathbf{x_1}$	$\mathbf{x_2}$	…	$\mathbf{x_n}$
$\mathbf{y_1}$	p_1c_{11}	0	…	0
$\mathbf{y_2}$	0	p_2c_{22}	…	0
.	.	.	.	.
$\mathbf{y_n}$	0	0	…	p_nc_{nn}
$\mathbf{y_{n+1}=S}$	p_1c_{1n+1}	p_2c_{2n+1}	…	p_nc_{nn+1}

Ehdollinen todennäköisyys $P(X|Y)$ on

$$p(x_i \mid y_j) = \frac{p(x_i)\,p(y_j \mid x_i)}{p(y_j)} = \frac{p_i c_{ij}}{v_j}.$$

Yhtälöiden L4.3 perusteella tiedetään, että $v_j = p_i c_{ij}$, kun $i = j$. Tällöin $P(x_i|y_j) = 1$ (kun $i = j$) ja ehdolliseksi todennäköisyysjakaumaksi saadaan:

	$\mathbf{x_1}$	$\mathbf{x_2}$	…	$\mathbf{x_n}$
$\mathbf{y_1}$	1	0	…	0
$\mathbf{y_2}$	0	1	…	0
.	.	.	.	.
$\mathbf{y_n}$	0	0	…	1
$\mathbf{y_{n+1}=S}$	$\frac{p_1c_{1n+1}}{v_{n+1}}$	$\frac{p_2c_{2n+1}}{v_{n+1}}$	…	$\frac{p_nc_{nn+1}}{v_{n+1}}$

Ehdollinen entropia on määritelty

$$H(X \mid Y) = \sum_{i,j} p(x_i, y_j) \log_2 \frac{1}{p(x_i \mid y_j)}. \qquad \text{(L4.4)}$$

Yllä esiteltyjen tulosten ja huomautuksen L4.1 perusteella voidaan todeta, että lauseke $p(x_i, y_j) \log_2 \frac{1}{p(x_i \mid y_j)}$ saa nollasta poikkeavia arvoja vain, kun $j = n+1$. Ehdollinen entropia riippuu siis vain symbolista $y_{n+1} = S$ ja voidaan näin ollen lausua

$$H(X \mid Y) = \sum_{i=1}^{n} p(x_i, y = S) \log_2 \frac{1}{p(x_i \mid y = S)}. \qquad \text{(L4.5)} \qquad \blacksquare$$

2. Esimerkki tiedustelujärjestelmän kapasiteetin laskemisesta

Emissioympäristön muodostaa viisi symbolia (lähetintä), jotka ovat toisistaan riippumattomia. Lähteen symbolijoukko on siis $A = \{a_1, a_2, a_3, a_4, a_5\}$. Esiintymistodennäköisyydet ympäristössä noudattelevat jakaumaa $P(A=a_i) = p_i$, $i = 1, \ldots, 5$. Todennäköisyydet $p_1 - p_4$ ovat 0.143 ja p_5 on 0.428. Lähteen todennäköisyysvektoriksi voidaan näin ollen asettaa

$$P_A = \begin{pmatrix} p_1 & p_2 & p_3 & p_4 & p_5 \end{pmatrix} = \begin{pmatrix} 0.143 & 0.143 & 0.143 & 0.143 & 0.428 \end{pmatrix}.$$

Lähteen entropiaksi saadaan

$$H_s(A) = \sum_{i=1}^{5} p(a_i)\log_2\frac{1}{p(a_i)} = 4\times\left(0.143\log_2\frac{1}{0.143}\right) + 0.428\log_2\frac{1}{0.428} = 2.128990\,\frac{bit}{symboli}$$

$$\approx 2.13\,\frac{bit}{symboli}\ . \qquad \text{(L4.6)}$$

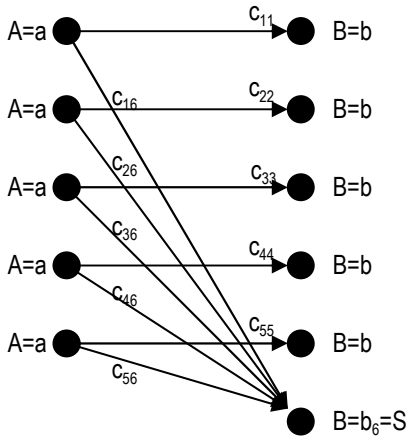
Oletetaan, että tiedustelujärjestelmän vastaanottaessa symboleita, symbolit $a1$ – $a4$ havaitaan todennäköisyydellä $P_{Hi} = 0.9$ (kun $i = 1 – 4$) ja symboli $a5$ havaitaan todennäköisyydellä $P_{H5} = 0.7$. Kun hyödyntämistodennäköisyyttä ei huomioida, voidaan kuvautumistodennäköisyydet määrittää yhtälöllä (ks. luku 4.3.3)

$$c_{ij} = \begin{cases} P_{Hi} & ,\text{kun } i = j \\ 1 - P_{Hi} & ,\text{kun } j = n+1. \\ 0 & ,\text{muulloin} \end{cases} \qquad \text{(L4.7)}$$

Kanavamatriisiksi **C** saadaan nyt

$$C = \begin{pmatrix} c_{11} & c_{12} & c_{13} & c_{14} & c_{15} & c_{16} \\ c_{21} & c_{22} & c_{23} & c_{24} & c_{25} & c_{26} \\ c_{31} & c_{32} & c_{33} & c_{34} & c_{35} & c_{36} \\ c_{41} & c_{42} & c_{43} & c_{44} & c_{45} & c_{46} \\ c_{51} & c_{52} & c_{53} & c_{54} & c_{55} & c_{56} \end{pmatrix} = \begin{pmatrix} 0.9 & 0 & 0 & 0 & 0 & 0.1 \\ 0 & 0.9 & 0 & 0 & 0 & 0.1 \\ 0 & 0 & 0.9 & 0 & 0 & 0.1 \\ 0 & 0 & 0 & 0.9 & 0 & 0.1 \\ 0 & 0 & 0 & 0 & 0.7 & 0.3 \end{pmatrix}. \qquad \text{(L4.8)}$$

Tilanne on kuvan L4.2 mukainen.



Kuva L4.2: Symbolien kuvautuminen kanavan yli.

Kerrotaan vektori $\mathbf{P_A}$ ja matriisi **C** keskenään ja saadaan vastaanottotodennäköisyydet $P(B=b_j)$ ja sitä vastaava todennäköisyysvektori v.

$$v = (v_j), \qquad \text{missä } v_j = \sum_{i=1}^{5} p_i c_{ij} \text{ ja } j = 1, 2, \ldots, 6.$$

Kuten edellä on todettu, ehdollinen entropia tässä tapauksessa riippuu vain symbolista $b_6 = S$. Jatkon kannalta ainut merkittävä alkio vastaanottotodennäköisyyksiä kuvaavassa vektorissa olisi v_6. Tässä esimerkissä esitetään kuitenkin laskelman kaikki välivaiheet.

$$v_1 = p_1c_{11} + p_2c_{21} + p_3c_{31} + p_4c_{41} + p_5c_{51} = p_1c_{11} = 0.143 \cdot 0.9 = 0.1287$$
$$v_2 = p_1c_{12} + p_2c_{22} + p_3c_{32} + p_4c_{42} + p_5c_{52} = p_2c_{22} = 0.143 \cdot 0.9 = 0.1287$$
$$v_3 = p_1c_{13} + p_2c_{23} + p_3c_{33} + p_4c_{43} + p_5c_{53} = p_3c_{33} = 0.143 \cdot 0.9 = 0.1287$$
$$v_4 = p_1c_{14} + p_2c_{24} + p_3c_{34} + p_4c_{44} + p_5c_{54} = p_4c_{44} = 0.143 \cdot 0.9 = 0.1287$$
$$v_5 = p_1c_{15} + p_2c_{25} + p_3c_{35} + p_4c_{45} + p_5c_{55} = p_5c_{55} = 0.428 \cdot 0.7 = 0.2996$$
$$v_6 = p_1c_{16} + p_2c_{26} + p_3c_{36} + p_4c_{46} + p_5c_{56} = 4 \times (0.143 \cdot 0.1) + 0.428 \cdot 0.3 = 0.1856$$

Eli. $v = (0.1287 \quad 0.1287 \quad 0.1287 \quad 0.1287 \quad 0.2996 \quad 0.1856)$ (L4.9)

Vastaanottotodennäköisyydet kertovat eri symboleiden suhteellisen jakauman vastaanotetussa symbolijonossa. Yllä olevasta nähdään, että riittävän pituisesta symbolijonosta on häiriöiden ja kohinan johdosta menetetty keskimäärin noin 18.6 % symboleista. Tämä ei kuitenkaan vielä kerro menetetyn informaation määrää. On huomattava, että tiedustelijan kannalta kiinnostavaa ei varsinaisesti ole se, kuinka paljon symboleita jäi vastaanottamatta, vaan se, mitä alun perin oli lähetetty puuttuvien symbolien paikalla (eli informaatio, joka menetettiin). Ehdollinen entropia kuvaa tilastollisesti juuri tätä asiaa. Ehdollisen entropian määrittämiseksi tulee laskea vielä yhteinen todennäköisyysjakauma $p(a_i,b_j)$ ja ehdollinen todennäköisyysjakauma $p(a_i|b_j)$.

Yhteinen todennäköisyysjakauma saadaan

$$p(a_i, b_j) = p(a_i)p(b_j \mid a_i) = p_i c_{ij}.$$

Tämä saa nollasta poikkeavat arvot vain kun $i = j$ tai $j = 6$. Yhteiseksi todennäköisyysjakaumaksi saadaan:

	a₁	**a₂**	**a₃**	**a₄**	**a₅**
b₁	$p_1c_{11} = 0.1287$	0	0	0	0
b₂	0	$p_2c_{22} = 0.1287$	0	0	0
b₃	0	0	$p_3c_{33} = 0.1287$	0	0
b₄	0	0	0	$p_4c_{44} = 0.1287$	0
b₅	0	0	0	0	$p_5c_{55} = 0.2996$
b₆	$p_1c_{16} = 0.0143$	$p_2c_{26} = 0.0143$	$p_3c_{36} = 0.0143$	$p_4c_{46} = 0.0143$	$p_5c_{56} = 0.1284$

Ehdolliseksi todennäköisyys lasketaan

$$p(a_i \mid b_j) = \frac{p(a_i, b_j)}{p(b_j)} = \frac{p(a_i)p(b_j \mid a_i)}{p(b_j)} = \frac{p_i c_{ij}}{v_j}.$$

Tämä lauseke saa jälleen nollasta poikkeavia arvoja vain, kun $i = j$ tai $j = 6$. Lisäksi on niin, että $p_ic_{ij} = v_j$, kun $i = j$. Tällöin $p(a_i|b_j) = 1$. Ehdolliseksi todennäköisyysjakaumaksi saadaan:

	$\mathbf{a_1}$	$\mathbf{a_2}$	$\mathbf{a_3}$	$\mathbf{a_4}$	$\mathbf{a_5}$
$\mathbf{b_1}$	1	0	0	0	0
$\mathbf{b_2}$	0	1	0	0	0
$\mathbf{b_3}$	0	0	1	0	0
$\mathbf{b_4}$	0	0	0	1	0
$\mathbf{b_5}$	0	0	0	0	1
$\mathbf{b_6}$	$\frac{p_1 c_{16}}{v_6} = 0.07705$	$\frac{p_2 c_{26}}{v_6} = 0.07705$	$\frac{p_3 c_{36}}{v_6} = 0.07705$	$\frac{p_4 c_{46}}{v_6} = 0.07705$	$\frac{p_5 c_{56}}{v_6} = 0.6918$

Yllä oleva jakauma siis kertoo, että mikäli vastaanotettu symboli oli esimerkiksi b_1 niin tällöin lähetetty symboli oli a_1 todennäköisyydellä 1. Tämä on helposti visuaalisesti hahmotettavissa myös kuvasta L4.2; symboliin b_1 ei suuntaudu vektoreita mistään muusta lähtöjoukon symbolista, kuin a_1. Jakaumasta nähdään myös, mikä todennäköisyys vastaa kutakin lähtöjoukon symbolia, kun on ”otettu vastaan” menetetty symboli (b_6).

Ehdollinen entropia on määritelty

$$H(A \mid B) = \sum_{i=1}^{5} \sum_{j=1}^{6} p(a_i, b_j) \log_2 \frac{1}{p(a_i \mid b_j)}. \qquad \text{(L4.10)}$$

Lauseen 5 ja huomautuksen L4.1 perusteella tiedetään, että ehdollista entropiaa ko. tapauksessa laskettaessa ei tarvitse huomioida muita tulojoukon symboleita, kuin b_6. Ehdollinen entropia on nyt

$$H(A \mid B) = \sum_{i=1}^{5} p(a_i, b_6) \log_2 \frac{1}{p(a_1 \mid b_6)} = 4 \times \left(0.0143 \log_2 \frac{1}{0.07705} \right) + 0.1284 \log_2 \frac{1}{0.6918}$$
$$= 0.27978 \frac{bit}{symboli} \approx 0.2798 \frac{bit}{symboli}. \qquad \text{(L4.11)}$$

Tiedustelujärjestelmän suhteellinen kapasiteetti on

$$D_R = H_s(A) - H(A \mid B) = 2.1290 \frac{bit}{symboli} - 0.2798 \frac{bit}{symboli} = 1.8492 \frac{bit}{symboli} \approx 1.85 \frac{bit}{symboli}. \qquad \text{(L4.12)}$$

Normalisoitu kapasiteetti on:

$$D_N = 1 - \frac{H(A \mid B)}{H_s(A)} = 1 - \frac{0.2798}{2.1290} \approx 0.869 \qquad \text{(L4.13)}$$

Tiedustelujärjestelmän saatavilla on näin ollen noin 87 % emissiomallin tuottamasta informaatiosta.

EHDOLLISEN ENTROPIAN SUURUUS SUHTEESSA EMISSIOMALLIN TUOTTAMAAN ENTROPIAAN

Määritelmä L5.1
Tiedustelujärjestelmän normalisoitu kapasiteetti on

$$D_N = 1 - \frac{H(X \mid Y)}{H_s(X)}, \qquad \text{(L5.1)}$$

missä $0 \le D_N \le 1$, koska aina pätee $H(X \mid Y) \le H_s(X)$.
Häiriöllisessä kuvautumistilanteessa pätee aina $D_N \in [0,1[$.

Määritelmä L5.2
Emissiomallit A_1 ja A_2 on määritelty identtisesti pois lukien niiden vakaat todennäköisyysjakaumat. Emissiomallin A_1 ominaisuuksia määrittää diskreetti todennäköisyysjakauma P_{A1} ja mallin A_2 todennäköisyysjakaumaa merkitään P_{A2}. Todennäköisyysjakaumien perusteella lasketuille entropioille pätee

$$H_s(P_{A1}) > H_s(P_{A2}). \qquad \text{(L5.2)}$$

Jatkossa merkitään $H_s(P_{A1}) = H_s^{A1}$ ja $H_s(P_{A2}) = H_s^{A2}$.

<u>Lause – Ehdollisen entropian suuruus suhteessa entropian suuruuteen</u>
Emissiomallien A_1 ja A_2 tuottama informaatio noudattelee määritelmän L5.2 olosuhteita. Oletetaan, että molempien mallien tuottamat informaatiot kuvautuu häiriöllisen kanavan yli samansuuruisella tiedustelujärjestelmän normalisoidulla kapasiteetilla eli

$$D_N^{A1} = D_N^{A2} = k \text{, missä } k \in [0,1[. \qquad \text{(L5.3)}$$

Tällöin ehdollisille entropioille on voimassa

$$H^{A1}(\cdot \mid \cdot) > H^{A2}(\cdot \mid \cdot). \qquad \text{(L5.4)}$$

<u>Todistus:</u>
Määritelmän L5.1 ja oletuksen L5.3 perusteella saadaan

$$D_N^{A1} = k = 1 - \frac{H^{A1}(\cdot \mid \cdot)}{H_s^{A1}} \quad \text{ja} \quad D_N^{A2} = k = 1 - \frac{H^{A2}(\cdot \mid \cdot)}{H_s^{A2}}. \qquad \text{(L5.5)}$$

Muokataan muotoon

$$H^{A1}(\cdot \mid \cdot) = H_s^{A1}(1-k) \quad \text{ja} \quad H^{A2}(\cdot \mid \cdot) = H_s^{A2}(1-k). \qquad \text{(L5.6)}$$

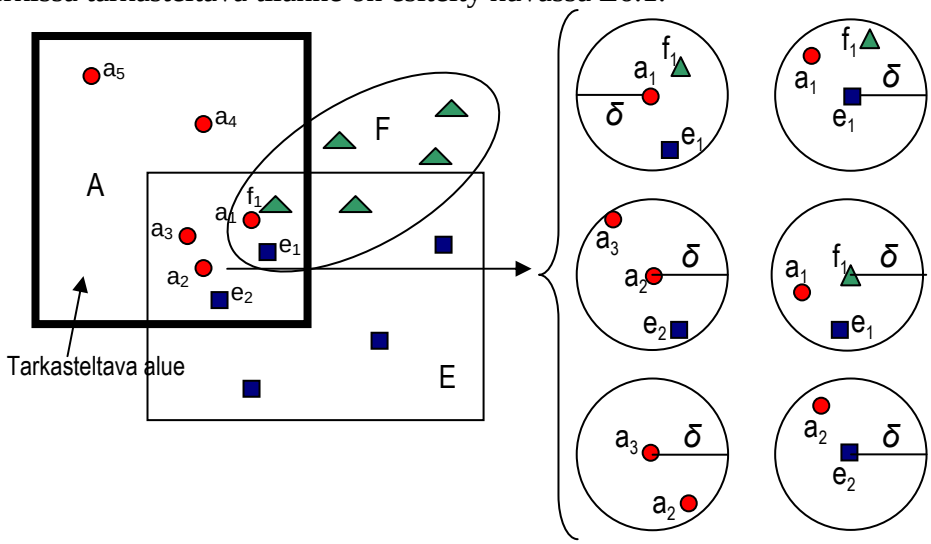
Määritelmän L5.2 perusteella saadaan

$$H^{A1}(\cdot \mid \cdot) = H_s^{A1}(1-k) > H_s^{A2}(1-k) = H^{A2}(\cdot \mid \cdot), \quad \forall\ k \in [0,1[. \qquad \text{(L5.7)}$$

Epäyhtälö L5.4 on todistettu. ■

ESIMERKKI HYÖDYNTÄMISTODENNÄKÖISYYDEN VAIKUTUKSESTA TIEDUSTELUJÄRJESTELMÄN SUHTEELLISEEN KAPASITEETTIIN

Esimerkissä tarkasteltava tilanne on esitelty kuvassa L6.1.



Kuva L6.1: Kolme limittynyttä osajoukkoa A, E ja F. Mikäli jokin toinen samaan lähetekategoriaan kuuluva symboli sijaitsee $\delta < 0.05\Delta$ etäisyydellä toisesta symbolista, on paikannus monikäsitteinen ja tämä on huomioitava kuvautumistodennäköisyyksissä.

Tarkastelun kohteena on osajoukko $A = \{a_1, a_2, a_3, a_4, a_5\}$, joka limittyy osittain osajoukon E ja F kanssa (ks. kuva yllä). Limittyvät symbolit ovat $E' = \{e_1, e_2\}$ ja $F' = \{f_1\}$. Oletetaan, että kaikkien osajoukkojen emissiomalleissa vierekkäisten symbolien valinnat ovat toisistaan riippumattomia. Oletetaan, että symboleiden esiintymistodennäköisyydet osajoukkonsa emissiomallissa ovat seuraavat:

$$P(A) = \left(\mu_{A(a1)}, \mu_{A(a2)}, \mu_{A(a3)}, \mu_{A(a4)}, \mu_{A(a5)}\right)$$
$$P(E') = \left(\mu_{E(e1)}, \mu_{E(e2)}\right)$$
$$P(F') = \mu_{F(f1)}$$

Oletetaan, että $\mu_{A(a5)} = 0.428$ ja kaikki muut esiintymistodennäköisyydet ovat 0.143. Lisäksi oletetaan, että symbolinopeudet $\varphi_A = \varphi_E = \varphi_F = 0.5$ symbolia/sek. Nyt voidaan muodostaa joukko α, joka sisältää kaikki tarkasteltavalle alueelle limittyneet symbolit ja jota vastaa todennäköisyysjakauma π. Olkoon siis

$$\alpha = \{\alpha_1 = a_1, \alpha_2 = a_2, \alpha_3 = a_3, \alpha_4 = a_4, \alpha_5 = a_5, \alpha_6 = e_1, \alpha_7 = e_2, \alpha_8 = f_1\}. \qquad \text{(L6.1)}$$

Todennäköisyysjakauma saadaan laskettua yhtälöllä (ks. luku 4.3.5 yhtälö 4.44)

$$\pi(\alpha_i) = \frac{\mu_{k(z)}\varphi_k}{\sum_{z\in\alpha}\mu_{k(z)}\varphi_k}, \qquad \text{missä } i = 1, \ldots, 8. \qquad \text{(L6.2)}$$

Summa $\sum_{z\in\alpha}\mu_{k(z)}\varphi_k = 7\cdot 0.143\cdot 0.5 + 0.428\cdot 0.5 = 0.7145$ ja nyt saadaan

$\pi(\alpha_1) = \pi(\alpha_2) = \pi(\alpha_3) = \pi(\alpha_4) = \pi(\alpha_6) = \pi(\alpha_7) = \pi(\alpha_8) = 0.1$ ja

$\pi(\alpha_5) = 0.3$.

Muodostetaan vastaava todennäköisyysvektori

$$\pi_\alpha = (\pi_1 \quad \pi_2 \quad \pi_3 \quad \pi_4 \quad \pi_5 \quad \pi_6 \quad \pi_7 \quad \pi_8) = (0.1 \quad 0.1 \quad 0.1 \quad 0.1 \quad 0.3 \quad 0.1 \quad 0.1 \quad 0.1).$$

Lähteen entropiaksi saadaan

$$H_s(\alpha) = \sum_{i=1}^{8} \pi(\alpha_i) \log_2 \frac{1}{\pi(\alpha_i)} = 7 \times \left(0.1 \log_2 \frac{1}{0.1} \right) + 0.3 \log_2 \frac{1}{0.3} = 2.8494 \frac{bit}{symboli}. \quad \text{(L6.3)}$$

Kohteiden paikantaminen tarkasteltavalla alueella ei ole kaikilta osin yksikäsitteistä, vaan osa symboleista sijaitsee alle δ etäisyydellä toisistaan (ks. kuva L6.1). Hyödyntämistodennäköisyys lasketaan yhtälöllä (ks. luku 4.3.3 yhtälö 4.30)

$$P_{EXi} = \frac{1}{m_i}, \qquad i = 1, 2, \ldots, 8. \qquad \text{(L6.4)}$$

Tässä m_i = symbolin α_i kanssa samaan kategoriaan kuuluvien ja etäisyydellä < δ sijaitsevien symboleiden, ml. symboli α_i itse, lukumäärä. Nyt saadaan (vertaa symbolijoukkoa L6.1 kuvaan L6.1)

$$P_{EXi} = (P_{EX1} \quad P_{EX2} \quad P_{EX3} \quad P_{EX4} \quad P_{EX5} \quad P_{EX6} \quad P_{EX7} \quad P_{EX8})$$
$$= \left(\frac{1}{3} \quad \frac{1}{3} \quad \frac{1}{2} \quad 1 \quad 1 \quad \frac{1}{3} \quad \frac{1}{2} \quad \frac{1}{3} \right).$$

Kun vielä oletamme, että havaitsemistodennäköisyys symbolille α_5 on 0.7 ja kaikille muille symboleille 0.9, niin voidaan määrittää käytettävyystodennäköisyydet (ks. luku 4.3.3 yhtälö 4.31)

$$P_{Ki} = P_{Hi} P_{EXi}, \qquad i = 1, 2, \ldots, 8. \qquad \text{(L6.5)}$$

Saadaan siis

$$P_{Ki} = (P_{K1} \quad P_{K2} \quad P_{K3} \quad P_{K4} \quad P_{K5} \quad P_{K6} \quad P_{K7} \quad P_{K8})$$
$$= (0.3 \quad 0.3 \quad 0.45 \quad 0.9 \quad 0.7 \quad 0.3 \quad 0.45 \quad 0.3)$$

Luvun 4.3.3 määrittelyn 4.32 mukaisesti kuvautumistodennäköisyydet ovat

$$c_{ij} = \begin{cases} P_{Ki} & , \text{kun } \exists \text{ mahdollisuus, että } x_i \mapsto y_j \text{ ja } j \neq n+1 \\ 1 - m_i P_{Ki} & , \text{kun } j = n+1 \\ 0 & , \text{muulloin} \end{cases}. \qquad \text{(L6.6)}$$

Kanavamatriisiksi **C** tulee nyt

$$C = \begin{pmatrix} c_{11} & 0 & 0 & 0 & 0 & c_{16} & 0 & c_{18} & c_{19} \\ 0 & c_{22} & c_{23} & 0 & 0 & 0 & c_{27} & 0 & c_{29} \\ 0 & c_{32} & c_{33} & 0 & 0 & 0 & 0 & 0 & c_{39} \\ 0 & 0 & 0 & c_{44} & 0 & 0 & 0 & 0 & c_{49} \\ 0 & 0 & 0 & 0 & c_{55} & 0 & 0 & 0 & c_{59} \\ c_{61} & 0 & 0 & 0 & 0 & c_{66} & 0 & c_{68} & c_{69} \\ 0 & c_{72} & 0 & 0 & 0 & 0 & c_{77} & 0 & c_{79} \\ c_{81} & 0 & 0 & 0 & 0 & c_{86} & 0 & c_{88} & c_{89} \end{pmatrix}$$

$$= \begin{pmatrix} P_{k1} & 0 & 0 & 0 & 0 & P_{K1} & 0 & P_{K1} & 1-3P_{K1} \\ 0 & P_{K2} & P_{K2} & 0 & 0 & 0 & P_{K2} & 0 & 1-3P_{K2} \\ 0 & P_{K3} & P_{K3} & 0 & 0 & 0 & 0 & 0 & 1-2P_{K3} \\ 0 & 0 & 0 & P_{K4} & 0 & 0 & 0 & 0 & 1-P_{K4} \\ 0 & 0 & 0 & 0 & P_{K5} & 0 & 0 & 0 & 1-P_{K5} \\ P_{K6} & 0 & 0 & 0 & 0 & P_{K6} & 0 & P_{K6} & 1-3P_{K6} \\ 0 & P_{K7} & 0 & 0 & 0 & 0 & P_{K7} & 0 & 1-2P_{K7} \\ P_{K8} & 0 & 0 & 0 & 0 & P_{K8} & 0 & P_{K8} & 1-3P_{K8} \end{pmatrix}$$

$$= \begin{pmatrix} 0.3 & 0 & 0 & 0 & 0 & 0.3 & 0 & 0.3 & 0.1 \\ 0 & 0.3 & 0.3 & 0 & 0 & 0 & 0.3 & 0 & 0.1 \\ 0 & 0.45 & 0.45 & 0 & 0 & 0 & 0 & 0 & 0.1 \\ 0 & 0 & 0 & 0.9 & 0 & 0 & 0 & 0 & 0.1 \\ 0 & 0 & 0 & 0 & 0.7 & 0 & 0 & 0 & 0.3 \\ 0.3 & 0 & 0 & 0 & 0 & 0.3 & 0 & 0.3 & 0.1 \\ 0 & 0.45 & 0 & 0 & 0 & 0 & 0.45 & 0 & 0.1 \\ 0.3 & 0 & 0 & 0 & 0 & 0.3 & 0 & 0.3 & 0.1 \end{pmatrix}.$$

Kerrotaan vektori π_α ja matriisi **C** keskenään ja saadaan vastaanottotodennäköisyydet $P(\beta_j)$ ja sitä vastaava todennäköisyysvektori v.

$v = (v_j)$, missä $v_j = \sum_{i=1}^{8} \pi_i c_{ij}$ ja $j = 1, \ldots, 9$.

Nyt saadaan

$$v_1 = \pi_1 c_{11} + \pi_2 c_{21} + \pi_3 c_{31} + \pi_4 c_{41} + \pi_5 c_{51} + \pi_6 c_{61} + \pi_7 c_{71} + \pi_8 c_{81} = 3 \cdot 0.1 \cdot 0.3 = 0.09$$
$$v_2 = \pi_1 c_{12} + \pi_2 c_{22} + \pi_3 c_{32} + \pi_4 c_{42} + \pi_5 c_{52} + \pi_6 c_{62} + \pi_7 c_{72} + \pi_8 c_{82} = 0.1 \cdot 0.3 + 2 \cdot 0.1 \cdot 0.45 = 0.12$$
$$v_3 = \pi_1 c_{13} + \pi_2 c_{23} + \pi_3 c_{33} + \pi_4 c_{43} + \pi_5 c_{53} + \pi_6 c_{63} + \pi_7 c_{73} + \pi_8 c_{83} = 0.1 \cdot 0.3 + 0.1 \cdot 0.45 = 0.075$$
$$v_4 = \pi_1 c_{14} + \pi_2 c_{24} + \pi_3 c_{34} + \pi_4 c_{44} + \pi_5 c_{54} + \pi_6 c_{64} + \pi_7 c_{74} + \pi_8 c_{84} = 0.1 \cdot 0.9 = 0.09$$
$$v_5 = \pi_1 c_{15} + \pi_2 c_{25} + \pi_3 c_{35} + \pi_4 c_{45} + \pi_5 c_{55} + \pi_6 c_{65} + \pi_7 c_{75} + \pi_8 c_{85} = 0.3 \cdot 0.7 = 0.21$$
$$v_6 = \pi_1 c_{16} + \pi_2 c_{26} + \pi_3 c_{36} + \pi_4 c_{46} + \pi_5 c_{56} + \pi_6 c_{66} + \pi_7 c_{76} + \pi_8 c_{86} = 3 \cdot 0.1 \cdot 0.3 = 0.09$$
$$v_7 = \pi_1 c_{17} + \pi_2 c_{27} + \pi_3 c_{37} + \pi_4 c_{47} + \pi_5 c_{57} + \pi_6 c_{67} + \pi_7 c_{77} + \pi_8 c_{87} = 0.1 \cdot 0.3 + 0.1 \cdot 0.45 = 0.075$$
$$v_8 = \pi_1 c_{18} + \pi_2 c_{28} + \pi_3 c_{38} + \pi_4 c_{48} + \pi_5 c_{58} + \pi_6 c_{68} + \pi_7 c_{78} + \pi_8 c_{88} = 3 \cdot 0.1 \cdot 0.3 = 0.09$$
$$v_9 = \pi_1 c_{19} + \pi_2 c_{29} + \pi_3 c_{39} + \pi_4 c_{49} + \pi_5 c_{59} + \pi_6 c_{69} + \pi_7 c_{79} + \pi_8 c_{89} =$$
$$= 7 \cdot 0.1 \cdot 0.1 + 0.3 \cdot 0.3 = 0.16$$

Eli $v = [0.09 \quad 0.12 \quad 0.075 \quad 0.09 \quad 0.21 \quad 0.09 \quad 0.075 \quad 0.09 \quad 0.16]$.

Ehdollisen entropian määrittämiseksi tulee laskea vielä yhteinen todennäköisyysjakauma $p(\alpha_i,\beta_j)$ ja ehdollinen todennäköisyysjakauma $p(\alpha_i|\beta_j)$.

Yhteinen todennäköisyysjakauma on

$$p(\alpha_i, \beta_j) = p(\alpha_i)\, p(\beta_j \mid \alpha_i) = \pi_i c_{ij},$$

jolloin saadaan:

	α_1	**α_2**	**α_3**	**α_4**	**α_5**	**α_6**	**α_7**	**α_8**
β_1	$\pi_1 c_{11} = 0.03$	0	0	0	0	$\pi_6 c_{61} = 0.03$	0	$\pi_8 c_{81} = 0.03$
β_2	0	$\pi_2 c_{22} = 0.03$	$\pi_3 c_{32} = 0.045$	0	0	0	$\pi_7 c_{72} = 0.045$	0
β_3	0	$\pi_2 c_{23} = 0.03$	$\pi_3 c_{33} = 0.045$	0	0	0	0	0
β_4	0	0	0	$\pi_4 c_{44} = 0.09$	0	0	0	0
β_5	0	0	0	0	$\pi_5 c_{55} = 0.21$	0	0	0
β_6	$\pi_1 c_{16} = 0.03$	0	0	0	0	$\pi_6 c_{66} = 0.03$	0	$\pi_8 c_{86} = 0.03$
β_7	0	$\pi_2 c_{27} = 0.03$	0	0	0	0	$\pi_7 c_{77} = 0.045$	0
β_8	$\pi_1 c_{18} = 0.03$	0	0	0	0	$\pi_6 c_{68} = 0.03$	0	$\pi_8 c_{88} = 0.03$
β_9	$\pi_1 c_{19} = 0.01$	$\pi_2 c_{29} = 0.01$	$\pi_3 c_{39} = 0.01$	$\pi_4 c_{49} = 0.01$	$\pi_5 c_{59} = 0.09$	$\pi_6 c_{69} = 0.01$	$\pi_7 c_{79} = 0.01$	$\pi_8 c_{89} = 0.01$

Ehdollinen todennäköisyys lasketaan

$$p(\alpha_i \mid \beta_j) = \frac{p(\alpha_i, \beta_j)}{p(\beta_j)} = \frac{p(\alpha_i)\, p(\beta_j \mid \alpha_i)}{p(\beta_j)} = \frac{\pi_i c_{ij}}{v_j}\,.$$

Ehdolliseksi todennäköisyysjakaumaksi saadaan:

	α_1	**α_2**	**α_3**	**α_4**	**α_5**	**α_6**	**α_7**	**α_8**
β_1	0.33	0	0	0	0	0.33	0	0.33
β_2	0	0.25	0.375	0	0	0	0.375	0
β_3	0	0.4	0.6	0	0	0	0	0
β_4	0	0	0	1	0	0	0	0
β_5	0	0	0	0	1	0	0	0
β_6	0.33	0	0	0	0	0.33	0	0.33
β_7	0	0.4	0	0	0	0	0.6	0
β_8	0.33	0	0	0	0	0.33	0	0.33
β_9	0.0625	0.0625	0.0625	0.0625	0.5625	0.0625	0.0625	0.0625

Ehdollinen entropia on (huom: logaritmien kantaluku on 2)

$$H(\alpha \mid \beta) = \sum_{i=1}^{8}\sum_{j=1}^{9} p(\alpha_i, \beta_j) \log \frac{1}{p(\alpha_i \mid \beta_j)} = p(\alpha_1, \beta_1) \log \frac{1}{p(\alpha_1 \mid \beta_1)} + p(\alpha_1, \beta_6) \log \frac{1}{p(\alpha_1 \mid \beta_6)}$$
$$+ p(\alpha_1, \beta_8) \log \frac{1}{p(\alpha_1 \mid \beta_8)} + p(\alpha_1, \beta_9) \log \frac{1}{p(\alpha_1 \mid \beta_9)} + p(\alpha_2, \beta_2) \log \frac{1}{p(\alpha_2 \mid \beta_2)}$$
$$+ p(\alpha_2, \beta_3) \log \frac{1}{p(\alpha_2 \mid \beta_3)} + p(\alpha_2, \beta_7) \log \frac{1}{p(\alpha_2 \mid \beta_7)} + p(\alpha_2, \beta_9) \log \frac{1}{p(\alpha_2 \mid \beta_9)}$$
$$+ p(\alpha_3, \beta_2) \log \frac{1}{p(\alpha_3 \mid \beta_2)} + p(\alpha_3, \beta_3) \log \frac{1}{p(\alpha_3 \mid \beta_3)} + p(\alpha_3, \beta_9) \log \frac{1}{p(\alpha_3 \mid \beta_9)}$$
$$+ p(\alpha_4, \beta_4) \log \frac{1}{p(\alpha_4 \mid \beta_4)} + p(\alpha_4, \beta_9) \log \frac{1}{p(\alpha_4 \mid \beta_9)} + p(\alpha_5, \beta_5) \log \frac{1}{p(\alpha_5 \mid \beta_5)}$$
$$+ p(\alpha_5, \beta_9) \log \frac{1}{p(\alpha_5 \mid \beta_9)} + p(\alpha_6, \beta_1) \log \frac{1}{p(\alpha_6 \mid \beta_1)} + p(\alpha_6, \beta_6) \log \frac{1}{p(\alpha_6 \mid \beta_6)}$$
$$+ p(\alpha_6, \beta_8) \log \frac{1}{p(\alpha_6 \mid \beta_8)} + p(\alpha_6, \beta_9) \log \frac{1}{p(\alpha_6 \mid \beta_9)} + p(\alpha_7, \beta_2) \log \frac{1}{p(\alpha_7 \mid \beta_2)}$$
$$+ p(\alpha_7, \beta_7) \log \frac{1}{p(\alpha_7 \mid \beta_7)} + p(\alpha_7, \beta_9) \log \frac{1}{p(\alpha_7 \mid \beta_9)} + p(\alpha_8, \beta_1) \log \frac{1}{p(\alpha_8 \mid \beta_1)}$$
$$+ p(\alpha_8, \beta_6) \log \frac{1}{p(\alpha_8 \mid \beta_6)} + p(\alpha_8, \beta_8) \log \frac{1}{p(\alpha_8 \mid \beta_8)} + p(\alpha_8, \beta_9) \log \frac{1}{p(\alpha_8 \mid \beta_9)} =$$

$$= 0.03\log\frac{1}{0.33} + 0.03\log\frac{1}{0.33}$$
$$+ 0.03\log\frac{1}{0.33} + 0.01\log\frac{1}{0.0625} + 0.03\log\frac{1}{0.25}$$
$$+ 0.03\log\frac{1}{0.4} + 0.03\log\frac{1}{0.4} + 0.01\log\frac{1}{0.0625}$$
$$+ 0.045\log\frac{1}{0.375} + 0.045\log\frac{1}{0.6} + 0.01\log\frac{1}{0.0625}$$
$$+ 0.09\log\frac{1}{1} + 0.01\log\frac{1}{0.0625} + 0.21\log\frac{1}{1}$$
$$+ 0.09\log\frac{1}{0.5625} + 0.03\log\frac{1}{0.33} + 0.03\log\frac{1}{0.33}$$
$$+ 0.03\log\frac{1}{0.33} + 0.01\log\frac{1}{0.0625} + 0.045\log\frac{1}{0.375}$$
$$+ 0.045\log\frac{1}{0.6} + 0.01\log\frac{1}{0.0625} + 0.03\log\frac{1}{0.33}$$
$$+ 0.03\log\frac{1}{0.33} + 0.03\log\frac{1}{0.33} + 0.01\log\frac{1}{0.0625} =$$

$$= 0.0480 + 0.0480$$
$$+ 0.0480 + 0.04 + 0.06$$
$$+ 0.0397 + 0.0397 + 0.04$$
$$+ 0.0637 + 0.0332 + 0.04$$
$$+ 0 + 0.04 + 0$$
$$+ 0.0747 + 0.0480 + 0.0480$$
$$+ 0.0480 + 0.04 + 0.0637$$
$$+ 0.0332 + 0.04 + 0.0480$$
$$+ 0.0480 + 0.0480 + 0.04 = 1.1199 \frac{bit}{symboli}$$

Tiedustelujärjestelmän suhteellinen kapasiteetti on

$$D_R = H_s(\alpha) - H(\alpha \mid \beta) = 2.8494 \frac{bit}{symboli} - 1.1199 \frac{bit}{symboli} = 1.7304 \frac{bit}{symboli} \approx 1.73 \frac{bit}{symboli} \text{ .(L6.7)}$$

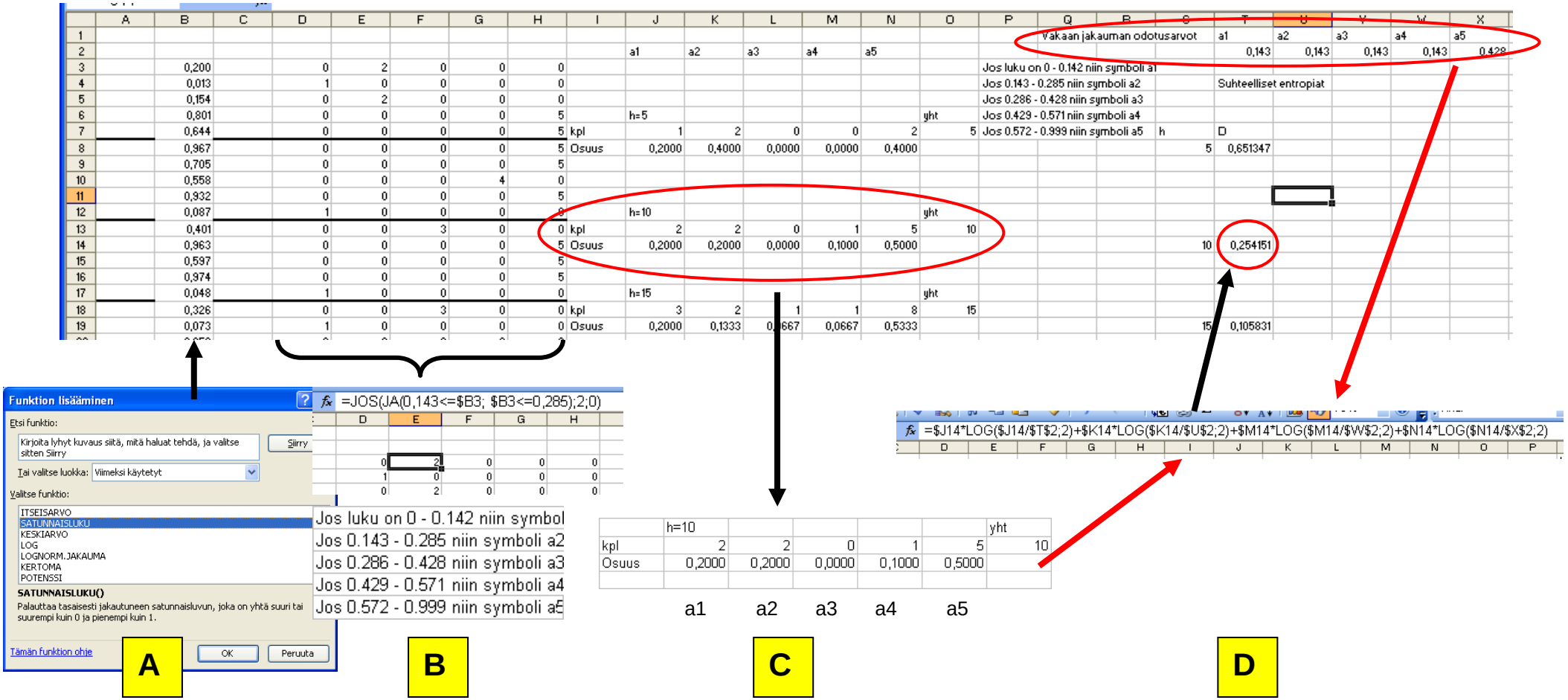
Normalisoitu kapasiteetti

$$D_N = 1 - \frac{H(\alpha \mid \beta)}{H_s(\alpha)} = 1 - \frac{1.1199}{2.8494} = 0.607 \text{ .} \qquad \text{(L6.8)}$$

Tiedustelujärjestelmän saatavilla on siis noin 61 % lähteen tuottamasta informaatiosta.

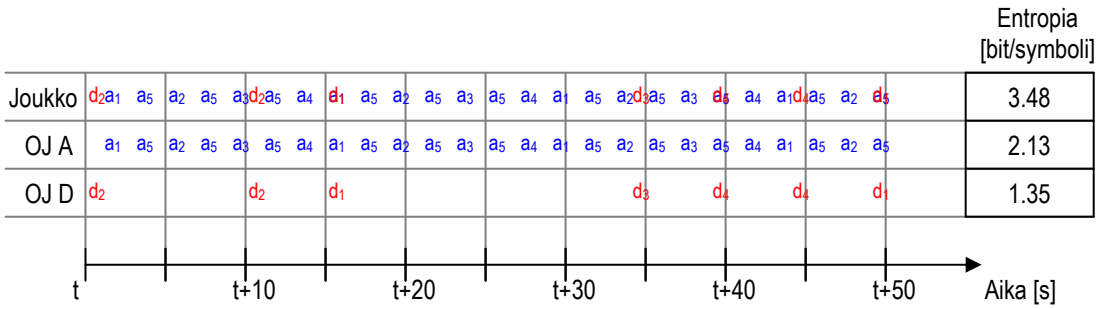
SUHTEELLISEN ENTROPIAN SIMULOINTI

Simuloinnit on toteutettu Microsoft Excel taulukkolaskentaohjelmalla alla esitettyä proseduuria noudattaen.
VAIHE A: Satunnaislukufunktion avulla arvotaan tasaisesti välille $[0,1[$ jakautunut satunnaisluku.
VAIHE B: Luokitellaan arvottu luku sitä vastaavaksi symboliksi tässä tapauksessa $a_1 - a_5$.
VAIHE C: Lasketaan muodostuneen symbolijonon tilastolliset todennäköisyydet jokaiselle symbolille $a_1 - a_5$. Laskenta on tehty kun symbolien yhteislukumäärä on ollut h = 5, 10, 15, 20, 25, 30, 35, 40, 45, 50, 60, 70, 80, 90 ja 100.
VAIHE D: Lasketaan suhteellinen entropia edellisessä vaiheessa muodostetun todennäköisyysjakauman sekä vakaan todennäköisyysjakauman välillä.
Tulokset tallennetaan ja vaiheet toistetaan jotta saadaan useampi simulaatio samasta tilanteesta. Saadut tulokset on esitetty käyrästöinä työn tekstiosuudessa.
Kaikki simulaatiot on toteutettu samalla periaatteella vaihdellen vaiheen B luokitteluparametreja ja symboleiden määriä tilanteen vaatimalla tavalla.



ESIMERKKI JOUKON ENTROPIAN MÄÄRITTÄMISESTÄ

Oletetaan, että joukko koostuu kahdesta toisistaan riippumattomasta osajoukosta A ja D, joiden ominaisuudet ovat samat, kuin on esitelty esimerkissä 4.5. Tilannetta vastaa kuva L8.1, josta ilmenee myös koko joukon entropia, joka on laskettu osajoukkojen entropioiden summana.



Kuva L8.1: Riippumattomien osajoukkojen A ja D tuottamat symbolijonot ja niiden yhteistuloksena aikaansaatu koko joukon symbolijono. Koko joukon entropia on osajoukkojen entropioiden summa. Osajoukkojen A ja D ominaisuudet esimerkissä 4.5 esitetynlaiset.

Koko joukon entropian määrittäminen aikaan sidottuna ei ole aivan yhtä suoraviivaista, kuin symbolikohtaisen entropian laskeminen. Seuraavassa esimerkissä on selvennetty asiaa.

Tarkasteluajan (50 sek) puitteissa osajoukko A tuottaa keskimäärin 25[1] symbolia ja osajoukko D keskimäärin 7[2] symbolia. Voidaan todeta, että osajoukkojen erikseen tarkastelujakson aikana tuottamien informaatioiden summa ei ole sama, kuin tilannetta koko joukkona tarkasteltaessa

$$25symb \cdot 2.13\frac{bit}{symb} + 7symb \cdot 1.35\frac{bit}{symb} = 62.7bit \neq 32symb \cdot 3.48\frac{bit}{symb} = 111.4bit\,. \qquad \text{(L8.1)}$$

Osajoukoille erikseen määriteltyjä aikaan sidottuja entropioita ei siis voi sellaisenaan laskea yhteen. Aikaan sidotut tarkastelut on syytä aina tehdä koko joukolle, jossa entropia on määritelty symbolikohtaisesti. Mikäli käsitellään entropiaa yksikössä bit/sekunti, on huomattava, että tällöinkään ei päädytä oikeaan tulokseen laskemalla suoraan yhteen erillisen osajoukkojen entropioiden nopeudet. Koko joukon symbolinopeus on osajoukkojen symbolinopeuksien summa. Yllä olevaan tilanteeseen sitoen saadaan esimerkiksi

$$\varphi^{AD} = \varphi^{A} + \varphi^{D}_{AVG} = 0.5\frac{symb}{s} + 0.14\frac{symb}{s} = 0.64\frac{symb}{s}\,. \qquad \text{(L8.2)}$$

Koko joukon entropian nopeus on:

$$H'_{AD} = \varphi^{AD} H_s^{AD} = 0.64\frac{symb}{s} \cdot 3.48\frac{bit}{symb} = 2.2272\frac{bit}{s} \approx 2.23\frac{bit}{s}\,. \qquad \text{(L8.3)}$$

Tämän perusteella todetaan edelleen, että 50 sekunnin aikana tuotetun informaation määrä on noin 111.4 bittiä, joka on sama kuin kohdassa L8.1 laskettu.

[1] Symbolinopeus x aika = 0.5 symb/s x 50 s = 25 symbolia
[2] Keskim. symbolinopeus x aika = 0.14 symb/s x 50 s = 7 symbolia

TIEDUSTELUJÄRJESTELMÄN SUHTEELLISEN KAPASITEETTI OSAJOUKOLLE D

Osajoukon D emissioympäristö muodostuu symbolijoukosta $D = \{d_1, d_2, d_3, d_4\}$. Emissiomalli on esimerkissä 4.5 ja liitteessä 3 esitetynlainen.

Lisäksi oletetaan, että symboli d_1 on radiohiljaisuudessa. Muut symbolit havaitaan todennäköisyydellä $P_{Hi} = 0.8$ ($i = 2, 3, 4$). Hyödyntämistodennäköisyyttä ei huomioida. Kanavamatriisi saadaan nyt muotoon

$$C = \begin{pmatrix} c_{11} & c_{12} & c_{13} & c_{14} & c_{15} \\ c_{21} & c_{22} & c_{23} & c_{24} & c_{25} \\ c_{31} & c_{32} & c_{33} & c_{34} & c_{35} \\ c_{41} & c_{42} & c_{43} & c_{44} & c_{45} \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0.8 & 0 & 0 & 0.2 \\ 0 & 0 & 0.8 & 0 & 0.2 \\ 0 & 0 & 0 & 0.8 & 0.2 \end{pmatrix}.$$

Emissiomallin vakaaksi todennäköisyysjakaumaksi muodostuu (ks. liite 3) vektorina esittäen

$$\mu = (\mu_1 \quad \mu_2 \quad \mu_3 \quad \mu_4) = (0.28 \quad 0.35 \quad 0.17 \quad 0.21).$$

Kerrotaan vektori **μ** ja matriisi **C** keskenään ja saadaan vastaanottotodennäköisyydet $P(B=b_j)$ ja sitä vastaava todennäköisyysvektori v.

$v = (v_j)$, missä $v_j = \sum_{i=1}^{4} \mu_i c_{ij}$ ja $j = 1, \ldots, 5$.

Koska symbolit voivat kuvautua vain itseään vastaaviksi tulojoukon symboleiksi tai välilyönneiksi, ainoa merkitsevä vastaanottotodennäköisyys on v_5 (vrt. liite 4). Saadaan:

$$v_5 = \mu_1 c_{15} + \mu_2 c_{25} + \mu_3 c_{35} + \mu_4 c_{45} = 0.28 \cdot 1 + 0.35 \cdot 0.2 + 0.17 \cdot 0.2 + 0.21 \cdot 0.2 = 0.426$$

Yhteistodennäköisyysarvot yhdistelmille joissa esiintyy symboli b_5:

	d_1	**d_2**	**d_3**	**d_4**
b_5	$\mu_1 c_{15}$ $= 0.28$	$\mu_2 c_{25}$ $= 0.07$	$\mu_3 c_{35}$ $= 0.034$	$\mu_4 c_{45}$ $= 0.042$

Ehdolliset todennäköisyydet yhdistelmille, joissa esiintyy symboli b_5:

	d_1	**d_2**	**d_3**	**d_4**
b_5	$\frac{\mu_1 c_{15}}{v_5}$ $= 0.6573$	$\frac{\mu_2 c_{25}}{v_5}$ $= 0.1643$	$\frac{\mu_3 c_{35}}{v_5}$ $= 0.0798$	$\frac{\mu_4 c_{45}}{v_5}$ $= 0.0986$

Lasketaan ehdollinen entropia

$$H(D \mid B) = \sum_{i=1}^{4} p(d_i, b_5) \log_2 \frac{1}{p(d_1 \mid b_5)} = 0.28 \log_2 \frac{1}{0.6573} + 0.07 \log_2 \frac{1}{0.1643}$$

$$+0.034\log_2\frac{1}{0.0798}+0.042\log_2\frac{1}{0.0986}=0.6163\,\tfrac{bit}{symboli}.$$

Tiedetään, että emissiomallin entropia on

$$H_s(D)=1.3545\,\tfrac{bit}{symboli}.$$

Tiedustelujärjestelmän suhteellinen kapasiteetti on nyt

$$D_R=H_s(D)-H(D\mid B)=1.3545\,\tfrac{bit}{symboli}-0.6163\,\tfrac{bit}{symboli}=0.7382\,\tfrac{bit}{symboli}\approx 0.74\,\tfrac{bit}{symboli}.$$

Tiedustelujärjestelmän normalisoiduksi kapasiteetiksi saadaan

$$D_N=1-\frac{0.6163}{1.3545}=0.545.$$

Tiedustelujärjestelmän saatavilla on siis noin 54.5 % tuotetusta informaatiosta.